AVAR

2022

CYBERSECURITY COUNTER PUNCH

1st - 2nd December 2022
Singapore

AVAR 25
ANNUAL CONFERENCE - 2022

PARTNERS

Platinum Sponsor

ESET Digital Security Progress. Protected.

Gold Sponsor

GETVISIBILITY OWN YOUR DATA

Silver Sponsors

CYBER THREAT ALLIANCE

CISCO TALOS

AV comparatives

T-Shirt Sponsor

SE Labs INTELLIGENCE-LED TESTING

Internet Sponsor

ReasonLabs

Delegate Kit Sponsor

K7 SECURITY

Media Sponsor

AV-TEST The Independent IT-Security Institute Magdeburg Germany

Supporting Sponsors

AhnLab AppEsteem®

NetApp® | Redington SEAMLESS PARTNERSHIPS

赛可达实验室 skd labs

Media Partners

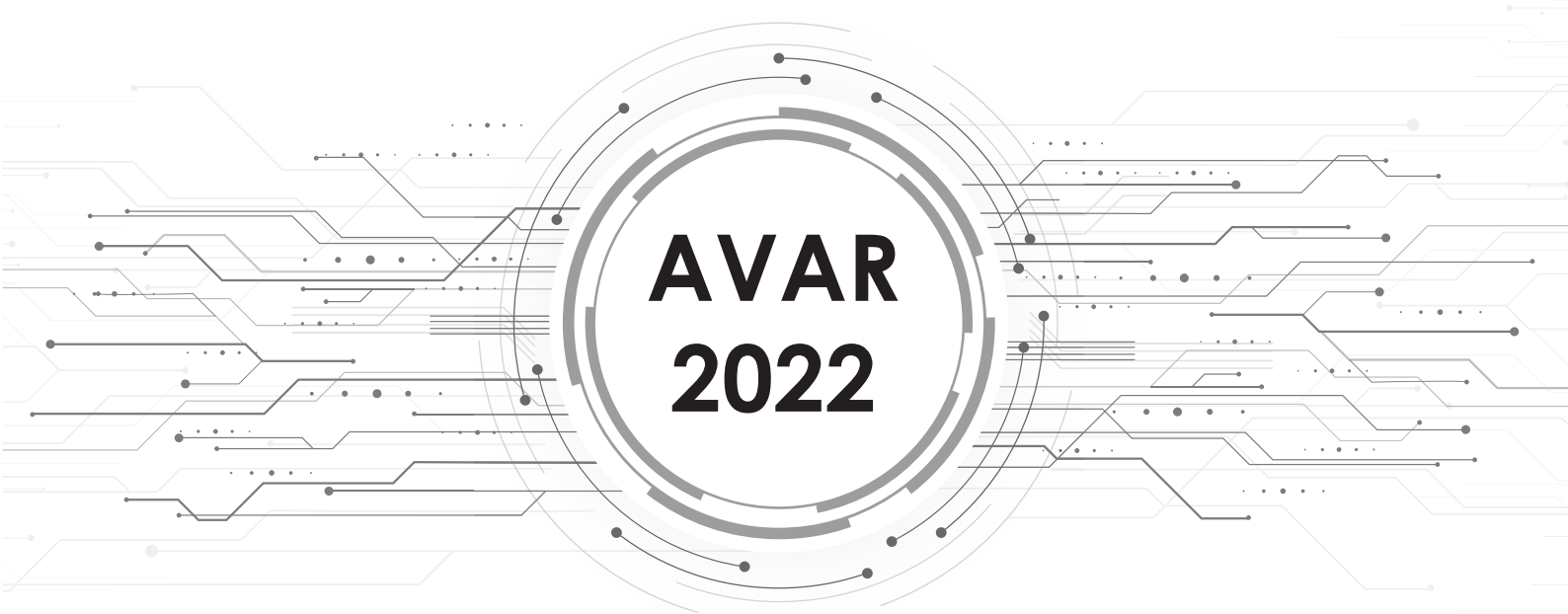
CYBER DEFENSE MAGAZINE

FRONTIER ENTERPRISE

Cyber CSA

CONTENTS

CONTENTS



CEO MESSAGE

I warmly welcome our speakers, delegates, partners, sponsors, and volunteers to AVAR 2022. This is the first time we are meeting in person since the pandemic began, and I am glad that we get to meet so many of you as building personal relationships is critical to fostering cybersecurity cooperation.

AVAR 2022 is the 25th edition of AVAR's annual international conferences, and also marks our shift to our new headquarters: AVAR is now based in Singapore to play a greater role in enhancing regional cybersecurity. AVAR's rising prominence is also reflected in the theme of this year's conference which is Cybersecurity Counter Punch. The pandemic triggered an unprecedented increase in cyberattacks which has affected individuals, organizations, and nations, and all of us will continue to play an important role in suppressing the rising tide of cyberthreats.

Threat actors are formidable adversaries. They are resourceful and highly motivated to pursue diverse goals ranging from financial gain to cyberwarfare. In this environment, creating effective cyber defenses will require threat researchers and management to act in concert towards achieving shared objectives. AVAR 2022 will promote such collaboration by serving as a forum that discusses threat research and also appeals to corporate leaders; the CISO Awards will recognize CISOs who have achieved exceptional advancement in cybersecurity in their organizations, and CISO Connect will feature CISO-oriented knowledge sessions including a panel discussion among CISOs.

A great deal of cybersecurity knowledge will be shared at AVAR 2022 through 45 presentations, 3 panel discussions, and 60 speakers from 21 countries. I am encouraged by the international participation, the expertise of the speakers, and the enthusiasm of the delegates as these indicate that the passion for defending the digital world is as strong as ever and our cyber future is in safe hands.

I welcome you again to AVAR 2022 and look forward to learning and working together to secure the infrastructure on which our digital civilisation is being built. Here's to another great conference.

Kesavardhanan J
CEO of AVAR


PROTECT
ADVANCED
Best-in-class endpoint protection against ransomware & zero-day threats, backed by powerful data security
• Prevent zero-day threats
• Protect business data
• Secure computers, mobiles and file servers
• Enjoy easy-to-use management
Cloud or on-prem deployment
Advanced threat defense
Endpoint protection
File server security
Full disk encryption
Learn more at www.eset.com/sg

AGENDA

DAY 1 Wednesday, 30th November, 2022

Time	Activity
16:00 – 18:00	Registration
18:30 – 21:00	Welcome Drinks Reception

DAY 2 Thursday, 1st December, 2022

Time	Track 1
9:00 – 9:30	Registration
9:30 - 10:40	Opening of Conference, Keynote speech(es) Kesavardhanan J, CEO of AVAR Dr. Pavan Duggal, Advocate, Supreme Court of India & Chairman, International Commission on Cyber Security Law Mr. Steven SIM, President, ISACA SG Chapter Mr. PK Gupta, Global CTO & APJC Presales Lead, Global Alliances Presales at Dell Technologies
10:40 – 11:00	Refreshment Break

Time	Track 1	Time	Track 2
11:00 – 11:30	**Twisted Panda: attacks against the Russian defense sector** Alexandra Gofman, David Driker **Check Point**	11:00 – 11:30	**DSE, KDP And Everything In Between: Novel Techniques To Run Unsigned Rootkits** Omri Misgav **Fortinet**
11:30 – 12:00	**SparklingElf, recent supplies to SparklingGoblin's Linux malware arsenal, new ties to APT41** Vladislav Hrčka **ESET**	11:30 – 12:00	**Operation Dragon Castling: Suspected APT Group Hijacks WPS Office Updater to Target East Asian Betting companies** Luigino Camastra, Igor Morgenstern **Avast**
12:00 – 12:30	**SMS PVA: how infected smartphones are used to register fake accounts** Ryan Flores **Trend Micro**	12:00 – 12:30	**Taohuawu, A much more sophisticated evolution from WHQL signed NetFilter rootkit** Robert Xiang Wang, Imran Khan **NortonLifeLock**
12:30 – 13:45	Lunch		

DAY 2 Thursday, 1st December, 2022

Time	Track 1	Time	Track 2
13:45 – 14:15	**TA505, Dridex and Squid Game** Kihong Kim, **SANDS Lab** Bomin Choi, **KISA**	13:45 – 14:25	**Panel Discussion – Cybersecurity Trends for 2023 and Beyond** Yul Bahat, **Kiteworks** Ajay Kumar, **CrowdStrike** Anil Malekani, **Microsoft** Rudy Lim, **Accenture Security**
14:15 – 14:45	**Earth Berberoka: An Analysis of a Multivector and Multiplatform APT Campaign Targeting Online Gambling Sites** Jaromir Horejsi **Trend Micro**	14:25 – 14:45	**Full Attack Chain Testing – How to test any security product usefully** Simon Edwards **SE Labs**
14:45 – 15:15	**XLLing in Excel – the world of malicious add-ins** Vanja Svajcer **Cisco Talos**	14:45 – 15:15	**Spoofing Microsoft M365 service to bypass most of the email security protections** Reegun Richard Jayapaul **Trustwave**
15:15 – 15:35	Refreshment Break		
15:35 – 16:05	**Panel Discussion - The Curse of the False Positive** Stefan Haselwanter, **AV-Comparatives** Robert Neumann, **Acronis** Evgeny Vovk, **Kaspersky** Vanja Svajcer, **Cisco** Righard Zwienenberg, **ESET** Eddy Willems, **G Data** Samir Mody, **K7 Computing**	15:35 – 16:05	**Who's swimming in South Korean waters? Meet ScarCruft's Dolphin** Filip Jurčacko **ESET**
16:05 – 16:35	**Sha Zhu Pan : The Cryptocurrency cocktail that started in Asia but is conquering the world** Jagadeesh Chandraiah, Xinran Wu **Sophos**	16:05 – 16:35	**Guard My Windows** Anurag Shandilya **K7 Computing**
16:35 – 17:05	**CFGDump: A tool for generic unpacking of polymorphic packed binaries** Craciun Vlad Constantin, Andrei Catalin Mogage **Bitdefender**	16:35 – 17:05	**Surviving the Era of Active Directory Attacks through in-Network defense** Chintan Shah **Trellix**
17:05 – 17:35	**Indian Power Sector targeted with latest LockBit 3.0 variant** Sathwik Ram Prakki **Quick Heal**	17:05 – 17:35	**eCrime – A Coming of Age Tale** Aaron Aubrey Ng **CrowdStrike**
19:15 – 20:00	Pre-dinner Drinks		
20:00 – 22:00	Gala Dinner		

DAY 3 Friday, 2nd December, 2022

Time	Track 1
10:00 – 10:30	**Keynote address: ♫ You ain't seen nothing yet ♫** Righard Zwienenberg **ESET** Eddy Willems **G DATA**
10:30 -11:00	**The Story of Jian – How APT31 Stole and Used an Unknown Equation Group 0-Day** Itay Cohen, Israel Gubi **Check Point**
11:00 -11:20	Refreshment Break

Time	Track 1	Time	Track 2
11:20 – 11:50	**Lazarus declares war on Windows system monitoring** Peter Kálnai, Matěj Havránek **ESET**	11:20 – 11:50	**Hitching a ride with Mustang Panda** Adolf Středa, Luigino Camastra, **Avast**
11:50 -12:20	**Aoqin Dragon – Newly-Discovered Chinese-linked APT Has Been Quietly Spying On Organizations For 10 Years** Joey Chen **SentinelOne**	11:50 -12:10	**CONTI Leaks: Behind the curtain of ransomware operations** Michael Abramzon, Sergey Shykevich **Check Point**
12:20 – 12:40	**Crawlector: A Threat Hunting Framework** Mohamad Mokbel **Trend Micro**	12:10 – 12:30	**Behind the MirrorFace mask: LODEINFO malware interfering with Japanese elections** Dominik Breitenbacher **ESET**
12:40 – 13:55	Lunch		
13:55 – 14:25	**MAIMLA: Make artificial intelligence machine learning again (Sponsor Presentation)** Filip Mazan **ESET**	13:55 – 14:10	**Using AI/ML to Build Effective Data Security Programs (Sponsor Presentation)** Ronan Murphy **Getvisibility**
14:25 – 14:45	**Story of new Attack Framework** Chetan Raghuprasad **Cisco Talos**	14:10 – 14:50	**Panel Discussion – Is the CISO the Next New Board Member?** Victor Keong, **Cohesity** Ashish Thapar, **NTT** Dr. Tan Kian Hua, **PCCW Solutions Limited/Lenovo** Vishal Sharma, **Kroll** Boris Hajduk, **Tokopedia** Dennis Batchelder, **AppEsteem**
14:45 – 15:15	**"WIN-P9NRMH5G6M8" – Transparent Tribe Perussian** Arun Kumar Shunmuga Sundaram, Rajeshkumar R **K7 Computing**	14:50 – 15:10	**INSECURE SECURITY UPDATE : Launching Counter Attacks with Cyber Awareness Campaigns Magniber Ransomware New Delivery Technique** John Karlo D. Agon, Lovely Jovellee Lyn B. Antonio **G DATA**

DAY 3 Friday, 2nd December, 2022

Time	Track 1	Time	Track 2
15:15 – 15:35	**Security-reducing Apps: a Call to Action** Hong Jia, Dennis Batchelder **AppEsteem**	15:10 – 15:30	**From Red to Black and Beyond – Evolution of a ransomware strain** Robert Neumann, Albert Zsigovits **Acronis**
15:35 – 15:50	**You have to see it to disrupt it: Mapping the Cyber Criminal Ecosystem (Sponsor Presentation)** Michael Daniel **Cyber Threat Alliance**	15:30 – 15:50	**Streamlining Threat Detections by Operationalising Sigma into SIEM Detections Automatically** Aashiq Ramachandran **Cyware Labs**
15:50 – 16:10	Refreshment Break		
16:10 – 16:40	**Summary of Linux kernel security protections and attack** Shubham Dubey **Microsoft**	16:10 – 16:25	**Lazarus and the tale of three rats (Sponsor Presentation)** Vitor Ventura **Cisco Talos**
		16:25 – 16:45	**Threat Hunting in M365 Environment** Thirumalai Natarajan **Mandiant**
16:40 – 17:10	**Threat Hunting of CrimsonRAT from APT36 group** Amey Gat **Fortinet**	16:45 – 17:10	**If The Hype Doesn't Kill You, Flawed or Missing Analysis Will** Randy Abrams **SecureIQLab**
17:10 – 17:15	Closing ceremony		
17:15 – 18:15	AVAR AGM / Members Meeting		

Solution

Getvisibility's AI powered data security platform supercharges data protection, control and visibility against data breaches and threats. Customers benefit from operational efficiencies, increased speed of deployment and significant cost reduction. Our machine-readable structured data can be used to create actionable insights through automatic association with information resources. The solution delivers meaningful visibility into the information assets within and across your enterprise, reducing risk, improving compliance, and enabling you to achieve optimal performance across your entire business.

LEGACY DATA

Getvisibility Focus

Discovery and classification of unstructured legacy data and access to the Getvisibility Reporting Suite

DATA IN CREATION AND ON ENDPOINTS

Getvisibility Synergy

End user classification on creation with AI suggestions and user activity reporting

ORGANISATIONAL OVERVIEW

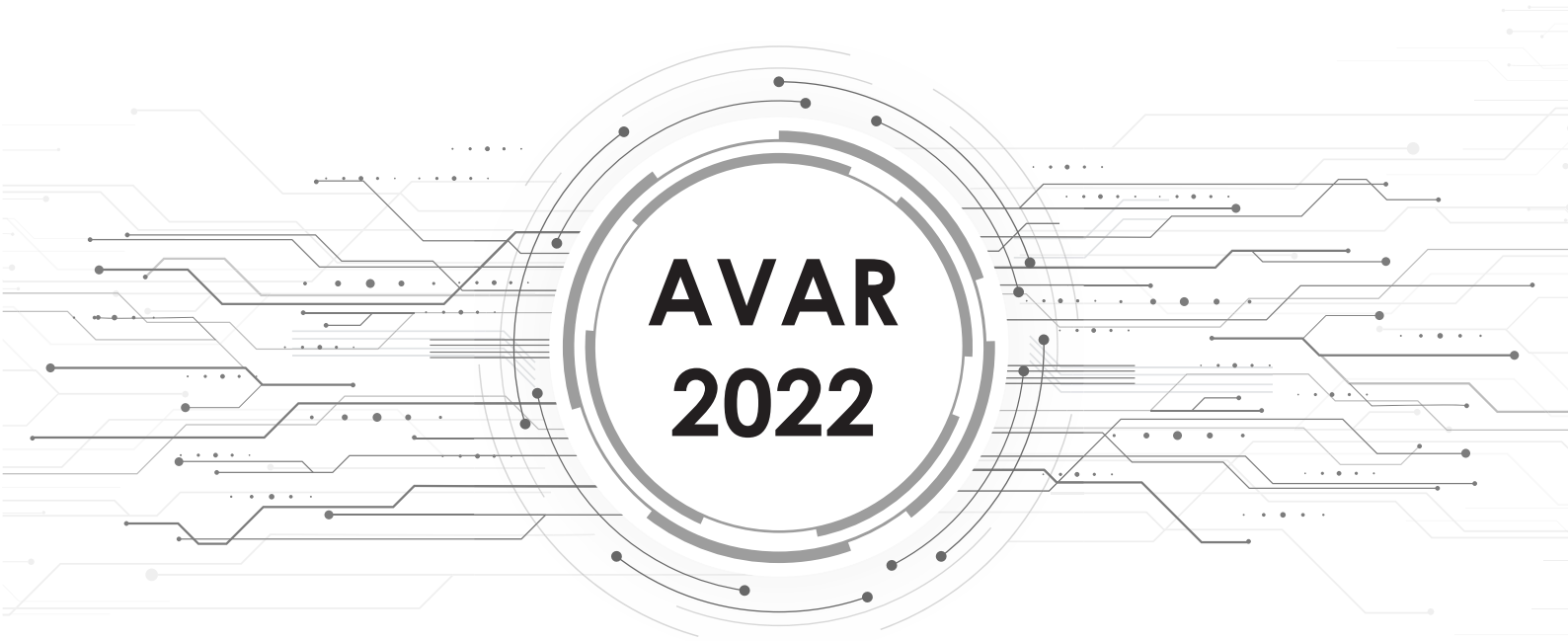
Getvisibility Protect Surface

Multi-layered reporting analysing the current data risk posture of an organization under multiple categories

Key Benefits

1. **PROTECT SURFACES**
   Define and protect your attack surfaces based on the conditions of your critical data
2. **DATA HYGIENE**
   Reduce your attack surface by finding, classifying & cleaning your data.
3. **LEAST PRIVILEGES**
   - Reduce access
   - Continuously monitor
   - Implement alerts
   - Align sensitive & privileged data
4. **ENHANCE DLP**
   Greater classification and data tagging enables a stronger more accurate Data Loss Prevention Solution. Ready to deploy out-of-the-box configuration
5. **INCIDENT ANALYSIS**
   Damage assessment in the wake of a cyber incident. What data was compromised and by whom?
6. **DATA TRACKING**
   Track & classify dynamic data, implement alerts on sensitive data Implement regulatory alignment ISO, CMMC, CCPA, HIPAA, ITAR EAR

www.getvisbility.com
contact@getvisibility.com
+1 866-326-5055



SPEAKERS/AUTHORS AND ABSTRACTS

TWISTED PANDA: ATTACKS AGAINST THE RUSSIAN DEFENSE SECTOR

Abstract:

The war started by Russia in Ukraine in February 2022 has significantly changed the geopolitical climate in the world, prompting the governments to focus their intelligence and cyber capabilities on Eastern Europe and Russia in particular. As situational awareness during armed conflicts involves gathering intelligence on motivations, tactics, plans, and military information on the forces and weapons from all the major political forces, it comes as no surprise that these actions might be carried out against friendly countries as well.

A month into the war, Check Point researchers detected what appears to be a sequence of attempts by a Chinese espionage actor to deploy advanced malware to the networks belonging to several Russian defense research institutes, primarily focused on electronic warfare and military-specialized radio-electronic equipment. These attacks used social engineering tricks exploiting the subject of sanctions, imposed as a result of the war by western countries on multiple Russian businesses, including the military and defense sector. Each of these attempts used different methods for initial infection, including MS Office documents with macros, LNK files, and, interestingly, Word documents exploiting 0-day vulnerability, unknown at the time.

In our talk, we will start by presenting the findings from our investigation into this cluster of activity against Russian defense institutes - which we called Twisted Panda - including the infection flows and technical analysis of the observed malicious stages and payloads. Then, we will go over this threat actor's history of malicious activity traced back to March 2021, and show the evolution of their techniques and tools. Lastly, we will talk about attribution and the actor's motivation behind going after those targets.

Alexandra Gofman
Check Point

Bio:

Alexandra Gofman has seven years of diverse background in cybersecurity in technical and customer-facing positions. Alexandra now leads Threat Intelligence Analysis Team at Check Point Research, focused on APT attacks, malware analysis and cyber threat intelligence.

David Driker
Check Point

Bio:

David Driker is a Security Researcher focusing on Malware Research at Check Point Research. David joined Check Point in 2019 and before that he was a Full Stack Developer for 5 years. David's research includes a mix of Malware research of cybercrime and Advanced Persistent Threat campaigns. When not researching malware he enjoys casual gaming and reading.

DSE, KDP AND EVERYTHING IN BETWEEN: NOVEL TECHNIQUES TO RUN UNSIGNED ROOTKITS

Abstract:

Code Integrity is a threat protection feature first introduced by Microsoft over 15 years ago. On x64-based versions of Windows, kernel drivers must be digitally signed and checked each time they are loaded into memory. This is also referred to as Driver Signature Enforcement (DSE). To overcome this restriction, attackers use valid digital certificates, either issued to them or they stole, or disable DSE during runtime instead. Obtaining a certificate is a logistical obstacle but tampering on the other hand is a technical challenge. Recent years prove the latter tactic only grew in popularity by various APTs as they continued to leverage the well-known DSE tampering technique.

Meanwhile, Microsoft rolled out new mitigations: driver blocklists and Kernel Data Protection (KDP), a new platform security technology for preventing data-oriented attacks. Since using blocklist only narrows the attack vector, we focused on how KDP was applied in this case to eliminate the attack surface.

We'll present two novel techniques we found to bypass KDP-protected DSE. Furthermore, they work on all Windows versions, starting with the first release of DSE. Each technique will be demonstrated on live machines. We'll also suggest a mitigation to cope with the issue, building upon the same premises as attackers, until HVCI becomes prevalent and really eliminates this attack surface.

Omri Misgav
Fortinet

Bio:

Omri has over a decade of experience in cyber-security. He serves as the CTO of a security research group at Fortinet focused on OS internals, malware and vulnerabilities and spearheads development of new offensive and defensive techniques. Prior to Fortinet, Omri was the security research team leader at enSilo. Before that, He led the R&D of unique network and endpoint security products for large-scale enterprise environments and was part of an incident response team, conducting investigations and hunting for nation-state threat actors.

SPARKLINGELF, RECENT SUPPLIES TO SPARKLINGGOBLIN'S LINUX MALWARE ARSENAL, NEW TIES TO APT41

Abstract:

StageClient is a configurable and modular Linux backdoor that we observed while investigating a targeted attack against a Hong Kong university in July 2021. Surprisingly, we discovered that the backdoor exhibits a huge functionality overlap with the Specter IoT botnet malware, a modular Linux RAT, that creates an indisputable link between the malware authors, meaning we can now say they come both from the same threat actor. More recently, we found strong connections between StageClient and SideWalk – a modular Windows backdoor belonging to SparklingGoblin, which is an APT group that partially overlaps with APT41 and BARIUM. By digging further, we found out that both StageClient and Specter are actually Linux variants of SideWalk. The targeting aligns with SparklingGoblin's targeted verticals. Pivoting on the cryptographic artefacts of StageClient, we found multiple other samples, including a custom undocumented userland rootkit featuring several unique and interesting techniques. We consider all these tools to be part of SparklingGoblin's arsenal. During this presentation, we will first present the connections between StageClient and Specter, by showing the common functionalities. Next, we will present the SparklingGoblin APT group to the audience, outlining the verticals and countries that this group targets, as well as their toolset and modus operandi. We will briefly describe some of the code similarities we found between StageClient and SideWalk, including encryption schemes, communication protocols, and victims fingerprinting. We will also sum up some of the differences we found, including available backdoor commands, versioning, and its defense evasion capabilities. In the third part of the presentation, we will describe the Linux rootkit we discovered. We will explain how the rootkit, that operates in userland, injects into processes and hides its files and network connections to achieve stealthiness. We will finish the presentation by a summing up of our findings, taking conclusions regarding the attribution matter.

Vladislav Hrčka
ESET

Bio:

Vladislav Hrčka has been working as a Malware Researcher at ESET since 2017. His focus is on reverse engineering challenging malware samples and his research into sophisticated malware families resulted in several published articles and papers. Apart from that he dealt with some fascinating obfuscation techniques used in malware and developed tools that can overcome them during his career. He has presented results of his work at several well-known conferences such as Black Hat USA, REcon, SecTor, CodeBlue, BSidesMTL and AVAR. He is soon going to finish his master's degree studies of Computer Science with a focus on cyber security at the Comenius University in Bratislava. Additionally, he teaches course Principles of Reverse Engineering at the local universities. In his spare time, he occasionally participate in various CTFs and enjoys sports, especially biking and swimming.

OPERATION DRAGON CASTLING: SUSPECTED APT GROUP HIJACKS WPS OFFICE UPDATER TO TARGET EAST ASIAN BETTING COMPANIES

Abstract:

Operation Dragon Castling is a suspected APT supply chain attack against East Asian betting companies that exploited a previously unknown vulnerability in WPS Office's updater to deliver malware to target Microsoft Windows systems. In this presentation, we will discuss how we saw strange DNS resolution requests for a domain related to WPS Office, but that was not part of WPS Office's infrastructure. Our investigation into these resolution requests showed they were being made from devices running WPS Office, devices belonging to East Asian betting companies. Seeing this, we suspected we had found a supply chain attack against WPS Office, though we were unable to identify the infection vectors at first. We investigated further and found that one of the systems issuing the unusual DNS resolution requests contained several malicious DLLs loaded by side-loading. One of these DLLs was a robust and modular core module written in C++. Aside from being used for privilege escalation and persistence, it also provided backdoor access to infected devices. After more investigating, we found two infection vectors. In the first case, the attacker sent an email with an infected installer to the support team asking them to check for a bug in their software. The second case was more interesting - we presume that the attacker hijacked the WPS updater by exploiting a previously unknown vulnerability. We discovered a new vulnerability (CVE-2022-24934) in the WPS Office updater, wpsupdate.exe. The WPS updater is a part of the WPS Office installation, which has more than 1.2 billion installations around the world. This attack showed a vulnerability that put those users at risk. We have contacted the WPS Office team about the vulnerability (CVE-2022-24934), and it has since been fixed.

Luigino Camastra
Avast

Bio:

Luigino Camastra is a malware researcher at Avast focused on reverse-engineering PE files, identifying malware families, and hunting advanced persistent threat groups. He holds a master degree in Computer Science from Czech Technical University in Prague. Luigino has presented his research at Virus Bulletin conferences, AVAR, Botconf, MNSEC2020, and APWG. In his free time he enjoys playing futsal and CTF.

Igor Morgenstern
Avast

Bio:

Igor Morgenstern is a senior malware researcher and reverse engineer at Avast focusing on hunting advanced persistent threat groups. Igor has presented at conferences, including MNSEC2020.

Previous experience includes: vulnerability research of a variety of databases resulting in discovery of multiple zero-day vulnerabilities, computer forensics.

SMS PVA: HOW INFECTED SMARTPHONES ARE USED TO REGISTER FAKE ACCOUNTS

Abstract:

We currently live in a world where online identities are closely tied to our actual identities. One's email account can be tied up to a food delivery app, a ride-hailing app, or a social media app. We let these apps interact with our personal and physical space by using it to buy physical items, avail of real world services, or share our locations, hobbies and people we interact with to the rest of the world. Because of this, user account authenticity and integrity is paramount. Without it, we won't be able to trust if an account selling an item online is trustworthy, or if the car that is in front of you is really the one you booked through your ride hailing app. This is why platforms and services need to ensure a user account is created by an actual human and the most common way to accomplish this is through SMS verification during account creation.

SMS verification is a way to make sure a user account is tied to a working mobile number, with the assumption that the one creating the user account owns that active mobile number. However, malicious actors are findings ways to defeat this verification system in order to create fake user accounts that is then used for scams, spam campaigns or engage in inauthentic user behaviour. Our research dives into a group providing a service called SMS PVA (Phone Verified Accounts). This service is designed to defeat the SMS verification employed by apps and platforms during account creation, so nefarious actors can create accounts for their malicious purposes. Digging deeper, we found out this service is made possible because the group getting the SMS verification codes from thousands of infected Android phones. These are real phones, owned by real people, that is then registered to an online account without the phone owner knowing it. We were able to analyse the malicious Android plug-ins responsible for this as well as trace the domains and servers it reports to. We are also able to link the Android malware and its infrastructure to a group we believe is operating in China. We are able to gather statistics on which mobile phones are infected and from what region, as well as the apps and platforms that were affected by actors who availed of this SMS PVA service. The findings of our investigation challenges the effectiveness of SMS verification as the primary verification tool in creating user accounts. It also challenges the security of the Android software supply chain as our findings suggests the malicious plug-ins are installed due to a pre-existing compromise in the software update component of cheap white label phones. Finally, we have also seen the apps and platforms where fake accounts were created, and by virtue of matching.

Ryan Flores
Trend Micro

Bio:

Ryan Flores is currently the Senior Manager of the Forward-Looking Threat Research team in APAC. Ryan Flores has 20 years of experience in IT security under his belt. He has held various positions in Trend Micro, from antivirus engineering to malware sourcing and honeypot development. His current role requires him to research on botnets and cybercrime and underground activities

TAOHUAWU, A MUCH MORE SOPHISTICATED EVOLUTION FROM WHQL SIGNED NETFILTER ROOTKIT

Abstract:

COVID changed our life in many perspectives, some bad, some good, there are significant increase in online gaming market since start of COVID. Taohuawu is a rootkit targeting unofficial online game players, mainly Chinese speaking users. It's designed to monitor web browsers, redirect network traffic, install trusted root certificate to degrade system and network security, download and run shellcode and additional payload. Rootkit driver components usually designed to hide, to protect, to monitor, are commonly seen have limited but core functions implemented in driver file, and therefore have a considerably small file size.

Taohuawu, a game changer which implement most of its functions in kernel driver, has a significant increase in file size, from KBs to MBs, and the customized file protector it used make it even harder to analyse. In additional to various self-protection mechanism, Taohuawu consist at least 7 stage payloads and keep them updated since mid or late 2021. Furthermore, an undocumented method is discovered in recent variants to hack into kernel to install and load its driver.

This paper presents a detailed analysis of Taohuawu rootkit and discusses potential people/group behind this campaign.

Robert Xiang Wang
NortonLifeLock

Bio:

Robert is a security professional with 20 years experience, specialised in malware reverse engineering and analysis. He works as a Principal Threat Analysis Engineer for NortonLifeLock in Dublin, Ireland.

Imran Khan
NortonLifeLock

Bio:

Imran is a Sr Manager of Protection Labs and has more than a decade of experience in the security industry. He has an extensive background in threat research and intelligence, security operations, and security engineering

TA505, DRIDEX AND SQUID GAME

Abstract:

KISA (Korea Internet & Security Agency) is a government agency in Korea that carry out improvemnet of Internet, Information Security, and International Cooperation service about ICT. Specifically, it is running its KISC (Korea Internet Security Center), which is CERT as like to CISA in America, and takes role on prevention and countermeasure of cyber attacks targetting private sector's ICT infrastructure. It mainly is serving countermeasure and analysis of hacking incidents that occur in the private sector, and spreads "Alert-State" on detected threats to them. In addition, by operating the Cyber Security Big Data Center, it analyzes and processes the acquired accident data to create an AI dataset and shares it with the private sector, enabling it to carry out a variety of tasks, such as fostering intelligence in cyber security.

SANDS Lab is a provider of cyber threat intelligence in South Korea. It is also an affiliated member of the CTA (Cyber Threat Alliance). It offers a service called "malwares.com" that is collecting, analyzing, and sharing around 2 million of IoCs (Indicator of Compromise) that are collected every day on all over the world. During the past 18 years, almost 2 billion malware have been collected and analyzed, and it provides analysis report for 30 billion IoCs. It posseses a variety of AI-based profiling technologies including its technical know-how of static and dynamic malware analysis, and then offers Intelligence Information to around 900 local and international clients.

In 2021, the KISA and SANDS Lab collaborated on a project to build the AI-datase in order to research and develop artificial intelligence models applicable to Cyber Security. Over 800 million datasets (source data and meta data) have been built on malware and cyber security incidents, which have many uses in the modern cyber security technology. And now, we preparing open different of artificial intelligence models and the AI-dataset.

SANDS Lab developed "AI-based Binary Reverse Engineering-based Attacker, Attack Technique Profiling (DBP: Deep Binary Profiler)" while building the above the AI-dataset. And, we achieved NET (New Excellent Technology) certification from Korean government by acknowledging the technological superiority. This technology extracts and trains various function-based features extracted through the disassembly process from the various collected binaries, identifies how similar it is to the existing attack techniques based on the code-based features, and as a result, the technique is able to detect and prevent attacks and identify even an attacker who has implemented the technique. With the "DBP" technology and "datasets" that was built, we could find out the tracking information of different threat actors who are operating significant attack campaigns around the world. It is a representative case that we have tracked the "Dridex malwares" exploiting keywords of "Squid Game", a Korean Netflix series that became popular last October in the world. These attack groups have features using a technique so-called "social engineering" to spread malwares, which steals the personal information of a number of random people by exploiting the interests and social concerns of the victims. Sometimes they are called as TA575, but we also discovered something relations that in there could locate indicators like the Dridex-series samples dispersed by the TA505 attack group. So, we tried to analysis and trace the group of TA575 with our dataset and technology (DBP).

Consequently, we could infer that the attack campaign of Dridex distribution with the keyword "Squid Game" is associated with the TA505 attack group. To explain this inference, we present the technical genealogy by comparing the coding similarity between the malware samples used in the "Squid Game" campaign and the Dridex ones utilized by the TA505 group.

TA505, DRIDEX AND SQUID GAME

Kihong Kim
SANDS Lab

Bio:

Career

2004-present CEO and founder of SANDS Lab

2009 Yonsei University majoring in Computer Engineering

2015 Development and Launching of malwares.com

2016 Prime Minister's Commendation

2017 Cyber Threat Alliance Affiliate Members

2021 New Excellent Technology (NET) Certification "Binary Reverse Engineering based Attacker Profiling Technology"

2021 Ministry of Science and ICT Commendation

2022 New Excellent Technology (NET) Certification "Multidimensional Metadata Extraction Analysis based Non-executable Malware Profiling and Detection Technology"

Interests

- Malicious code analysis and tracking

- CTI Service Development

- Development of AI Technology in Cyber Security Area

Bomin Choi
KISA

Bio:

Bomin Choi is a cyber security big data center's researcher at KISA (Korea Internet & Security Agency) which is Korean government. She has not only studied on data science as like artificial intelligence, big data, and etc. for effective cyber threat response for last 10 years, but also interested in the research and development of malware profiling, and CTI.

In recent she is responsible for the project to build the cyber security AI-dataset, and she has an ambitious goals that it can be the best global AI-dataset as like KDD-Cup99 which is produced by DARPA in 1999. So she going to introduce about the backgrounds and meaning of the dataset and why we produce AI dataset, and etc. in AVAR 2022.

EARTH BERBEROKA: AN ANALYSIS OF A MULTIVECTOR AND MULTIPLATFORM APT CAMPAIGN TARGETING ONLINE GAMBLING SITES

Abstract:

Despite being illegal in some countries, global online gambling industry grows steadily year after year, flourishing during the global pandemic. This trend was not surprisingly noticed by advanced threat actors as we observed and analyzed campaigns targeting online gambling platforms.

In this research, we will focus on a multiplatform (Windows, Linux, and Mac) campaign involving known espionage tools as well as new malware families. Operated by individuals with knowledge of Chinese language, the victims of this campaign are mostly, but not limited to, online gambling customers in Southeast Asia.

We noticed some interesting infection vectors, such as exploitation of persistent cross-site scripting vulnerabilities in legitimate websites resulting in redirection to fake installers of popular applications, or a backdoored custom chat application, suggesting a very targeted campaign.

The delivered malware families are well known espionage tools such as PlugX and Gh0stRAT, or lesser known XNote and HelloBot. Some of these Linux malwares were previously reported for their cybercrime usage, but never for espionage purposes. We also found some previously unreported malware families dubbed oRAT and PuppetLoader, one of which uses images for payload storage. After carefully analyzing their unique features, we will highlight one interesting case where a flawed cipher implementation led us to the discovery of an additional malware likely implemented by the same threat actor.

As a conclusion, we will discuss the infrastructure and multiple links we found with known advanced threat actors and older investigations.

Jaromir Horejsi
Trend Micro

Bio:

Jaromir Horejsi is a threat researcher at Trend Micro. He specializes in hunting and reverse-engineering threats that target Windows and Linux. He has researched many types of threats over the course of his career, covering threats such as APTs, DDoS botnets, banking Trojans, click fraud and ransomware. He has successfully presented his research at RSAC, SAS, Virus Bulletin, HITB, FIRST, AVAR, Botconf and CARO.

FULL ATTACK CHAIN TESTING - HOW TO TEST ANY SECURITY PRODUCT USEFULLY

Abstract:

Security product testing can be useful to improve products and help customers make the most appropriate buying decisions. We look at what it means to test using the full attack chain, including the advantages in assessing full products and combinations of products, as well as the limitations and even dangers of taking realism too far. The presentation will include the following:

- Test environment considerations

- Introduction to the concepts of the attack chain and the alternative approach of atomic testing

- Case studies

- Ways to construct and present attack chains

- Testing like a real Advanced Persistent Threat (APT) in seven steps

- Dealing the products that don't cover the full attack chain

- Detection or protection testing?

- When realism gets a little too real... (unexpected interaction with criminals)

Simon Edwards
SE Labs

Bio:

Simon Edwards is the founder and CEO of SE Labs, a London-based company that specialises in advanced security testing. He provides tailored security advice to large businesses and more general technical advice to small businesses and individuals.

Simon focuses on cybersecurity and develops ways to test computer security products and services. He built and ran the world's first real-world anti-virus test and continues to innovate in testing that involves computer hacking.

A founder member of the Anti-Malware Testing Standards Organization (AMTSO), Simon was chairman of its Board of Directors between 2012 and 2015, and between 2017 and 2019. He is currently co-chair.

Simon features on the DE:CODED podcast, which provides different types of security advice for businesses and individuals, recognising that people need security in both their work and personal lives.

XLLING IN EXCEL – THE WORLD OF MALICIOUS ADD-INS

Abstract:

When Microsoft announced that they will prevent downloaded VBA macros from executing and users won't be able to work around that there was an audible sigh of relief in the anti malware researcher's community. For decades, VBA macros have been one of the main infection vectors employed by many actors, from commodity malware developers to cybercriminals and state sponsored groups. This change will be gradual as we will have to wait until most of the users upgrade to the latest versions of Microsoft Office. Nevertheless, it marks a step change in the malware resilience of Office applications even if take in account that security vulnerabilities will provide another port of entry for malicious code for the foreseeable future. VBA macros and vulnerabilities are not the only way for malicious code to interact with the rich capabilities of Microsoft Office and use Office programs to infect systems. For example, native Excel XLL add-ins, according to Microsoft, are files with extension .xll, a type of dynamic link library (DLL) file that can only be opened by Excel. XLL add-in files must be written in C or C++.

The C API has none of the higher-level rapid development features of Microsoft Visual Basic for Applications (VBA), COM, or the Microsoft .NET Framework. Memory management is low level, and therefore puts greater responsibility on the developer. Many Excel features that are exposed through COM, making them available through VBA and the .NET Framework, are not exposed to the C API. For malicious actors to run their code when Excel opens an XLL file, the XLL file must contain one of the well-known exported functions which will called when specific events in Excel are triggered. For example, xlAutoOpen, is called by Excel whenever the XLL is activated and xlAutoClose whenever the XLL is unloaded.

The development of XLL add-ins requires a level of proficiency in C/C++ programming which malware actors often don't possess so there are several builders that allow threat actors to build certain types of XLL without an in-depth programming knowledge and the API functions. There are other frameworks, such as Excel-DNA which allows easy creation of XLL files using .NET languages. Although XLL files have been used by malicious actors since their introduction by Microsoft, we have observed an increase in their usage since Microsoft announced the discontinuation of VBA macros, even if that decision was temporarily reverted.

In this presentation, we dive into the world of Microsoft Excell Add-ins and XLL malware. We start with the development process, the official tools such as Excel XLL SDK and the API available to Excel Add-Ins and continue with documenting other tools for building XLL files.

We discuss evolution of XLL samples since their inception and specifically focus on the most interesting examples indicating that the interest in XLL add-ins is not just in the domain of the most prevalent families of commodity malware.

We finish with recommendations on how to protect against XLL plugins and the best ways of detecting them.

Attendees of the session will obtain an in-depth knowledge about developing XLL files as well as information about malware families using them as infection vectors.

Vanja Svajcer
Cisco Talos

Bio:

Vanja Svajcer works as a Technical Leader at Cisco Talos. He is a security researcher with more than 20 years of experience in malware research and detection development. Prior to joining Talos, Vanja worked as a Principal Researcher for SophosLabs and led a Security Research Team at Hewlett Packard Enterprise.

Vanja enjoys tinkering with automated analysis systems, reversing binaries and analysing mobile malware. He thinks time spent scraping telemetry data to find indicators of new attacks is well worth the effort. He presented his work at conferences such as Virus Bulletin, RSA, CARO, AVAR, BalcCon and others.

In his free time, he is trying to improve his acoustic guitar skills and often plays basketball, which at his age is not a recommended activity

SPOOFING MICROSOFT M365 SERVICE TO SEND PHISHING EMAILS THAT WILL BYPASS EMAIL SECURITY PROTECTIONS

Abstract:

Using Microsoft M365 service, we can send a spear phishing email to the targeted users by bypassing email security protections. In this case, I demonstrated with Microsoft Safelinks, the key part is,

- The attacker doesn't need to host the payload elsewhere
- Don't need to create a domain
- Don't need to compromise other websites
- Don't need to compromise high reputation websites
- All the requirements can be obtained from the Microsoft M365 service to send a phishing payload
- The context I meant is not the end payload (SharePoint link), From the starting email delivery itself from the Microsoft M365 service

History:

- I found this technique and reported it to Microsoft in October 2019, but Microsoft rejected it as a non-security issue
- But from mid-year 2020 after the Covid starts, WFH is the normal working pattern and we have observed lots of successful Spear phishing campaigns started using Microsoft SharePoint as an end payload for credential harvesting or asking the victim to download the malware and so on
- Later by August 2021, we observed a huge trend related to this attack and recorded by most of the security vendors blog

What differs from the current attack trend?

So, I have decided to revisit, and I found the issue exists till now

- The main context I meant is not the end payload (SharePoint link) like what other adversaries are doing, my finding starts from the email delivery itself via the Microsoft M365 service
- I can create a free M365 typo squatting domain that matches the target organization and starts delivering the phishing email
- The important problem is, that this will bypass most of the Email-Security products
- Threat groups like TA505 can use this method successfully if they came to know of this technique because by default it will bypass the Email-Security products

SPOOFING MICROSOFT M365 SERVICE TO SEND PHISHING EMAILS THAT WILL BYPASS EMAIL SECURITY PROTECTIONS

Reegun Richard Jayapaul
Trustwave

Bio:

Reegun Richard is Senior Threat Architect @ SpiderLabs, Trustwave's threat research/hunting team; having 11 years of experience in Security Research, Malware analysis, Reverse Engineering, Threat Hunting, Incident Response, Security trainer; he has been working on clients with different sectors and doing threat hunting on multiple technologies and environments.

He is also doing offensive security on finding new vulnerabilities and reporting to vendors, improving the quality of deliverables from his research, simulating, and researching new attacks to build better detection, and the Main contributor to GoldenSpy and GoldenHelper analysis and findings, actively enhancing defensive skills from simulating offensive methodologies.

Previously worked in the financial sector and did Incident Response, Malware Analysis, and purple teaming; he worked in Symantec's elite threat research team 'MATI' and uncovered APT attacks related to PRC and DPRK threats, holding industry-standard certifications including Sans GREM, GCIA, OSCP.

WHO'S SWIMMING IN SOUTH KOREAN WATERS? MEET SCARCRUFT'S DOLPHIN

Abstract:

ScarCruft, also known as APT37 and Reaper, is an espionage group that has been operating since at least 2012. It primarily focuses on South Korea, but other Asian countries also have been targeted. ScarCruft seems to be interested mainly in government and military organizations, and companies in various industries linked to the interests of North Korea. Last year, ScarCruft conducted a watering-hole attack on a South Korean newspaper site. This attack was previously publicly described as having the BLUELIGHT backdoor as its final payload. However, we discovered a second, more sophisticated backdoor called Dolphin that was deployed on selected victims via BLUELIGHT.

Dolphin is a new, previously undocumented addition to ScarCruft's toolset. It supports a wide range of espionage capabilities – such as monitoring drives and portable devices and exfiltrating interesting files, or stealing credentials from browsers. Interestingly, it also provides the ability to lower the security of victims' Google and Gmail accounts. In line with ScarCruft's signature TTPs, Dolphin abuses cloud storage services for C&C communication. In this talk, we will present a technical description of the Dolphin backdoor and its capabilities. We will also provide useful information for threat hunters looking to track ScarCruft activity, including the evolution across multiple Dolphin versions that we have observed after our initial discovery.

Filip Jurčacko
ESET

Bio:

Filip Jurčacko is a Malware Researcher, working at ESET since 2015. Filip focuses on hunting and analyzing sophisticated threats. His research results in technical reports and improvements to detection capabilities. In his free time, he likes to improve skills in CTF competitions. He holds a master's degree in software engineering from Slovak University of Technology in Bratislava.

SHA ZHU PAN : THE CRYPTOCURRENCY COCKTAIL THAT STARTED IN ASIA BUT IS CONQUERING THE WORLD

Abstract:

We were contacted by a vulnerable user who lost around $85,000 investing in a fake app. When we started digging into this malware, we started to understand that this is a deeper rabbit hole that started in Asia and is spread worldwide. We have been contacted by several victims, including someone who lost up to a million dollar to this organized crime. In Sha Zhu Pan or also known as CryptoRom, the victims are singles who are looking for potential partners on dating sites. Crooks use stolen celebrity profiles and contact the victim out of the blue. They entice their victims by talking nicely and then moving the conversation to messaging apps like WhatsApp. They never disclosed their faces or met in person, citing Covid-19. After getting familiar and spending time with their new partners, they talk victims into trading and big investments, usually calling themselves investors or bankers. Victims are asked to install fake trading or cryptocurrency applications. Initially, crooks invest some money and let the victim make a profit. Once the victim starts believing them, they are asked to invest large amounts. To avoid tracing investment happens through Crypto apps like Binance. After this, they are never allowed to withdraw, repeatedly denied, or asked to invest more, citing fake taxes or fees. On the tech side, the crooks target both Apple iOS (Apps and Web Clips) and Android users. They create fake App store and Play store look-alike pages for downloads. To bypass the iOS app store, they use Apple Ad hoc distribution (Super signature), Enterprise program (Enterprise signature) using stolen certificates or Apple Test Flight feature (Test Flight signature) using third-party commercial services. Victims must click a link, then they walk through the entire process. On the web side, they create well-known trading app look-alike sites with real-time data obtained through real sites to convince users. We obtained a couple of bitcoin wallet addresses shared by victims with one linked to a $1.4 million total payment and another up to $464 million. This is a worldwide problem with several victims losing hundreds of thousands including someone who lost up to $1 million. We want to share our presentation with a wider audience to create awareness and increase research on this malware.

Jagadeesh Chandraiah
Sophos

Bio:

Jagadeesh Chandraiah is a senior malware researcher at SophosLabs, specializing in mobile malware analysis. Jagadeesh has been working at SophosLabs for over 10 years. Jagadeesh started working on Windows malware analysis and is currently focusing on mobile malware analysis. Jagadeesh has a Master's degree in computer systems security from the University of South Wales.

Jagadeesh likes to track malware, research and find novel ways to detect and remediate them. Jagadeesh is a frequent contributor to the SophosLabs Uncut blog and has written blog posts about several mobile malware topics. Jagadeesh also regularly presents his research at international security conferences and in the past has presented his research at DeepSec, AVAR, CARO, and Virus Bulletin.

Outside of work, Jagadeesh enjoys playing badminton.

SHA ZHU PAN : THE CRYPTOCURRENCY COCKTAIL THAT STARTED IN ASIA BUT IS CONQUERING THE WORLD

Xinran Wu
Sophos

Bio:

Xinran Wu graduated from the University of New South Wales in Australia. He has been working as a threat researcher at SophosLabs for over six years, where he has been reversing and analysing malware for various platforms. His current research areas include Mac threats, and also Android threats. Xinran enjoys reading and playing tennis in his free time

The Cyber Threat Alliance

The Cyber Threat Alliance (CTA) is a 501(c)(6) non-profit membership organization that is working to improve the cybersecurity of our global digital ecosystem by enabling our members to share high-quality cyber threat information at both human and machine speed; distribute critical defensive information and threat reports; and work in a trusted community. We don't just talk about threat intelligence sharing — we do it every day. We seek to:

Protect End Users

Members use our automated platform to share curated and actionable threat intelligence that can be deployed to their customers in near-real time. Members also share early warnings about research findings, enabling more effective defensive actions against malicious actors.

Disrupt Malicious Actors

CTA and its members create outputs, collaborate on actions, and respond to cyber incidents to reduce the overall effectiveness of malicious actors' tools and infrastructure.

Elevate Overall Security

CTA shares content, establishes partnerships, and promotes policies that enhance the overall security and resilience of the digital ecosystem.

What CTA Members Are Saying...

"CTA makes automated real-time actional threat intelligence sharing work. With today's threat landscape, this is critical. The CTA trusted community ensures communication is on-going and collaboration is regular and consistent. Other sharing organizations can't compete with this model." Jaya Baloo, CISO, Avast

"The best way to combat the negative impact of cybercriminals and best protect our customers is through cooperation and partnership based on actionable intelligence from diverse sources." Ken Xie, CEO, Fortinet

"The cybersecurity industry is built on trust, collaboration, and sharing. We see CTA as providing a unique platform to nurture those symbiotic relationships.", Samir Mody, VP Threat Research, K7 Computing

CYBER THREAT ALLIANCE

Interested in Membership?
Contact us: newmember@cyberthreatalliance.org

GUARD MY WINDOWS

Abstract:

The Windows LSA (Local Security Authority), responsible for user authentication and maintaining sensitive user data such as Windows logon passwords and access tokens, has always been the holy grail for exploitation in the hackers checklist for obvious reasons, and there has been much success in associated ventures to undermine it.

For example, recent user identity spoofing vulnerabilities reported in LSA, such as CVE-2022-26925 and CVE-2021-36942, allow attackers to authenticate to and own a Domain Controller (DC), compromising an entire organisation's network by calling the LSARPC (LSA-Remote Procedure Call) interface function with strategic parameters set up. DC is a server which responds to authentication requests in a domain and typically controls access to various resources within an organisation's LAN. Now, it turns out that CVE-2021-36942 was exploited by LockFile ransomware to allow it to push its payload to all networked clients using a compromised DC.

Further, OS Credential Dumping has been a part of attacker TTPs for ages. It works by extracting credentials from the LSASS service in the form of NTLM (NT LAN Manager) and SHA hashes, and, in some cases, even clear text. Easy availability of offensive tools such as Mimikatz has made it simple for mere script kiddies to extract credentials from the LSA.

Fortunately, of late, Microsoft has paid more attention towards these issues and has introduced features to mitigate such attacks against LSA. In addition to patching known vulnerabilities, other features introduced include Credential Guards - storing secrets in an isolated process supported by Virtualization Based Security, executing LSA as a protected process, and Attack Surface Reduction (ASR) rules. These features ensure that LSA and related processes execute with restricted privileges and prevent other processes from accessing the LSA. Nevertheless, despite these features in place, there yet exist ways to extract credential details even on Windows 11.

In this presentation, we shall deep dive into the Windows LSA service with a focus on its exploitation, past and present, using the modus operandi of password extraction tools, as well as our own demo exploitation of CVE-2022-26925 which leads to remote code execution. We will also explore the inner workings of recently introduced mitigations such as Credential Guard and ASR, and how they help to defend the critical LSA against exploitation and compromise.

Anurag Shandilya
K7 Computing

Bio:

Anurag Shandilya is the Assistant Vulnerability Research Manager at K7Computing's Threat Control Lab. His areas of research include Windows and IoT vulnerabilities. He has 7+ years of experience in Vulnerability Research and Vulnerability Assessment and Penetration Testing (VAPT). He has presented at AVAR (2018, 2020, and 2021), VB (2019) and CARO (2020) and actively contributes to the K7 Computing blog. His other areas of interest include bug bounty and playing table tennis.

CFGDUMP: A TOOL FOR GENERIC UNPACKING OF POLYMORPHIC PACKED BINARIES

Abstract:

Given the large amount of highly obfuscated and packed malicious binaries, reverse-engineers mandates for efficient ways to dig for de-obfuscated content. CFGDump is a fast dynamic mechanism to rebuild payloads and random memory dumps, back to full OS-related binary applications, including import tables and Entry Point, even though they were not available in the first place. While existing tools handle memory dumps in a standard way, CFGDump uses a CFG (Control Flow Graph) brute-force approach to recover the original Entry Point for payloads and unpacked pieces of code, as well as a CFG fingerprinting algorithm to spot the end of the unpacking sequence. Our tool is currently used to assist ransomware decryption with reliable content, starting from packed ransomware binaries.

Craciun Vlad Constantin
Bitdefender

Bio:

Vlad Craciun received his Ph.D. degree in Computer Science from the Romanian Institute "Alexandru Ioan Cuza University of Iasi". At the moment he is involved in automating the analysis of binary applications which implements analysis-evasion and at the same time he is an assistant professor at the same University, teaching various programming technologies. He joined Bitdefender Laboratories in early 2009, dealing with disinfection of file-infectors and cryptographic analysis of ransomwares. His current research interest includes binary instrumentation, symbolic/concolic execution, and control flow analysis.

Andrei Catalin Mogage
Bitdefender

Bio:

Andrei Mogage is a PhD student at the Alexandru Ioan Cuza University of Iași, Romania, studying formal methods applied in the cybersecurity field. He has joined Bitdefender in 2016 and has been involved in analysis and recovery of various cyber threats, with a keen focus on ransomware attacks. His current research interests include cryptography, malicious threats and exploitation

SURVIVING THE ERA OF ACTIVE DIRECTORY ATTACKS THROUGH IN-NETWORK DEFENCE

Abstract:

Post successful breach of the target network, attackers would categorically progress towards discovering the critical assets to exploit and exfiltrate data. During this process of lateral movement and expanding their footholds in the network by pivoting to multiple systems, attackers would look to probe the target network primarily for Active Directory systems. Active Directory is the prime targets for adversaries since it is the central repository for enterprise-wide user information, managing user authentication. Acquiring sufficient privileges to gain access to Active Directory and compromising it serves as a catalyst for the adversaries in executing further attacks. We have had many such high impact Privilege Escalation and Remote Code Execution vulnerabilities being exploited in Active Directory authentication protocols like Kerberos, Netlogon and RPC interfaces (like PrintNightMare) leading to complete domain takeover. Additionally Active Directory exposing huge attack surface, it is of paramount importance for enterprise networks to protect and mitigate attacks against Active Directory.

Coalescing production assets with the deceptive services can play a conclusive role in detecting and mitigating attacks in the domain environment once the production endpoint is compromised. Deceptive network alongside production network turns out to be highly effective approach in detecting lateral movement path towards critical assets including domain controllers. Building effective deception infrastructure that blends well with the production environment would require planting deceptive credentials in the production and decoy endpoints to detect initial enumeration attacks and the same time, injecting lures on the endpoints to build and deflect attacker's lateral movement path towards deceptive services.

During this talk, highlighting the AD attack surface, we will discuss about network deception as an approach to detect and mitigate Active Directory attacks and then progressively discuss on how we can build and achieve deceptive infrastructure including AD deception, which could potentially lead to early attack detection and mitigation.

Following are the key takeaways from the talk:

- Active Directory attack surface and impact
- Attacker's lateral movement path to Active Directory services
- Deception network approach for detecting lateral movement and AD attacks
- Building and achieving AD deception infrastructure for early attack detection

Chintan Shah
Trellix

Bio:

Chintan Shah is currently working as a Sr. Lead Security Researcher with Trellix Intrusion Prevention System and holds broad experience in the network security industry. He primarily focuses on Exploit and vulnerability research, building Threat Intelligence frameworks, Reverse engineering techniques and Malware Research. With multiple patent pending innovations in exploit detection, Chintan is a passionate blogger and speaker at many security research conferences. His interests lie in software fuzzing for vulnerability discovery, analysing exploits, malwares and translating them into product improvements.

INDIAN POWER SECTOR TARGETED WITH LATEST LOCKBIT 3.0 VARIANT

Abstract:

The top ransomware groups shift their target industry regularly based on their financial motives and vulnerable sectors. After the infamous Conti ransomware group was disbanded, the LockBit group has claimed dominance over other groups this year by working with various Initial Access Brokers. Conti's former members split up, joining already existing cybercrime groups and started to target energy and power sectors with a new unknown ransomware payload.

The intelligence derived by Quick Heal researchers had already identified the Energy and Power sector as a segment prone to cyberattacks and had increased the vigil on the same. This proactive monitoring proved fruitful soon after we identified one of the recent premium entities attacked in this segment. Our investigation and analysis determined that the new LockBit 3.0 ransomware variant caused the infection that exhibited huge anti-forensic activity with similarities from other variants.

As these ransomware groups increase and evolve with new techniques, an advance warning of these threats is needed to prevent the attacks more than ever. In this paper, we will cover the complete analysis and their attack chain leading to the ransomware payload and changes adopted to their extortion tactics.

Sathwik Ram Prakki
Quick Heal

Bio:

Sathwik Ram Prakki is working as a Security Researcher in Security Labs at Quick Heal. His focus areas are Threat Intelligence, Threat Hunting, and writing detections. He has a background in Offensive Security & Windows Internals and is keen on exploring new detection techniques through Reverse Engineering and Malware Research.

His previous experience at C-DAC under the Ministry of Electronics & IT gave a jumpstart in his cybersecurity career. He graduated from Osmania University in 2019 with a degree in Electronics & Communication and has also completed his Post Graduate Diploma in Embedded Systems & Design at C-DAC in 2020.

eCRIME – A COMING OF AGE TALE

Abstract:

In the early days of Ransomware, attacks were perpetrated primarily by single criminal entities. These adversaries operated independently and were responsible for developing tools to orchestrate an entire attack sequence. Fast forward to today, the eCrime ecosystem is vast and interconnected, with many criminal enterprises co-existing to support Big Game Hunting (BGH) Ransomware Operations. Notably, over the past two years, an emergent class of eCrime Adversaries known as Access Brokers developed a pivotal role in this ecosystem with providing initial access to a variety of Adversaries. During the same period, a number of dramatic shifts have been observed in the BGH space, including the exponential surge in the adoption of the Extortion and Data Leaks tactics, the proliferation of Ransomware-as-a-Service, the employment of Supply Chain compromises to scale the impact of a Ransomware attack, and more. This session will cover the history of this evolution, takes a deep dive into these recent threat trends, and strives to offer the audience with useful insights to better defend the organisation against eCrime.

Aaron Aubrey Ng
CrowdStrike

Bio:

Aaron Aubrey Ng is a Strategic Threat Advisor at CrowdStrike. He is responsible for CrowdStrike's Threat Intelligence business in the Asia Pacific and Middle East regions. Aaron supports organisations with the operationalisation of threat intelligence as part of their Cybersecurity strategy. As a Security Evangelist, Aaron frequently speaks at Security Conferences, sharing insights into the latest threat trends and developments. Aaron got his start in Security and Threat Intelligence in the Singapore Armed Forces as a Military Intelligence Officer. He concluded 12 years of Active Duty in 2019 and has served in multiple command appointments in classified intelligence units, and garnered staff experience in the areas of strategic planning and policy development. In his penultimate tour of duty, Aaron was instrumental in establishing the Defence Cyber Organisation (DCO), which is akin to Singapore's Cyber Command.

♫ YOU AIN'T SEEN NOTHING YET ♫

Abstract:

After "Oops! It Happened Again" and "Fool Us! Or is it us Fools?", the dynamic presentation duo sadly had to decide that once more they have to return. Since last year so many ludicrously avoidable cybersecurity incidents have been experienced that one really must wonder if users will ever learn. How much education and awareness does one need. It becomes even more cynical if the incidents are caused by the politicians that made the cyber-regulations but don't follow these (read: break) themselves "as they are inconvenient to work with". In their usual energetic and lively presentation style, this dynamic duo will present real-life examples of cyber-incidents, and explain what went wrong and how they could have been prevented. Eager to learn why we (the users) keep making these mistakes, they will also dive deeper into the reasons that history keeps repeating itself. And they will reveal the surprising common denominator that they have found. To get in the mood, turn on your Walkman, insert that 70's cassette, and play Bachman Turner Overdrive's "You ain't seen nothing yet" as loud as you can. Then, after watching our presentation, we hope everyone will stop making these errors so that we can genuinely say "Here's something that you're never gonna forget! B-b-b-baby"

Righard Zwienenberg
ESET

Bio:

Zwienenberg started dealing with computer viruses in 1988 after encountering the first virus problems at the Technical University of Delft. His interest thus kindled and studied virus behavior and presented solutions and detection schemes ever since. Initially starting as an independent consultant, in 1991 he co-founded CSE Ltd. In November 1995 Zwienenberg joined the Research and Development department of ThunderBYTE. In 1998 he joined the Norman Development team to work on the scanner engine. In 2005 Zwienenberg took the role of Chief Research Officer. After AMTSO – Anti Malware Testing Standards Organization - was formed, Zwienenberg was elected as president. He is serving on the board of AVAR and on the Technical Overview Board of the WildList. In 2011 Zwienenberg was looking for new opportunities and started as a Senior Research Fellow at ESET. In April 2012 Zwienenberg stepped down as President of AMTSO to take the role as CTO and later as CEO. In 2016 he rejoined the AMTSO board for another two-year run. He also is the Vice Chair of the Executive Committee of IEEE ICSG. In 2018, Zwienenberg joined the Europol European Cyber Crime Center (EC3) Advisory Group as an ESET representative.

Zwienenberg has been a member of CARO since late 1991. He is a frequent speaker at conferences – among these Virus Bulletin, EICAR, AVAR, FIRST, APWG, RSA, InfoSec, SANS, CFET, ISOI, SANS Security Summits, IP Expo, Government Symposia, SCADA seminars, etc. - and general security seminars. His interests are not limited to malicious code but have broadened to include general cybersecurity issues and encryption technologies over the past years.

♫ YOU AIN'T SEEN NOTHING YET ♫

Eddy Willems
G DATA

Bio:

Eddy Willems is a worldwide known cyber security expert from Belgium. He is a board member of 3 security industry organizations, EICAR, AVAR and LSEC, and is the resident Security Evangelist at G DATA Cyberdefense.

He became a founding member of EICAR in 1991, one of the world's first security IT organizations. Over the years he has served in many extra roles in different security industry organizations. Several CERTs, press agencies, print and online publications and broadcasting media, for example CNN, use his advice regularly. In October of 2013, he published his first book in Belgium and the Netherlands, entitled 'Cybergevaar' (Lannoo). A German translation followed afterwards and an English translation and update, Cyberdanger (Springer), was published in 2019. He is also co-author of the Dutch SF cyberthriller 'Het Virus' published in 2020. Eddy is a known inspiring speaker and is giving lectures and presentations (including TEDx) worldwide for a very diverse audience from children to experts.

THE STORY OF JIAN – HOW APT31 STOLE AND USED AN UNKNOWN EQUATION GROUP 0-DAY

Abstract:

At the beginning of 2017, the Chinese-affiliated APT31 was caught deploying a 0-Day exploit against a US-based company. A CVE was issued for the vulnerability, it got patched, case closed. Right?

Well, turns out this isn't exactly the case.

During their ongoing research of the exploits used by different malware and APT groups, our Malware and Vulnerability research teams stumbled upon a major revelation regarding this incident. While analyzing "Jian", the caught-in-the-wild APT31 exploit, they saw evidence connecting it to unfamiliar tools of another well-known actor - Equation Group.

Join us as we unearth a hidden exploitation framework used by Equation Group's DanderSpritz. This framework, named NtElevation, contains 4 different LPE exploits, of which the exploits code-named "EpMe" and "EpMo" were yet to receive any public attention. Not only so, but analysis of EpMe revealed it to be an exploit for the same vulnerability later used by APT31.

Coincidence? We think not.

In our talk, we compare Jian and EpMe, and show the vast similarity between the two. Taking into account the fingerprints of both actors, the evidence at hand points at a remarkable scenario - APT31 captured and adapted an unknown Equation Group 0-Day exploit for their own use, years before the Shadow Brokers leak reached the headlines."

Itay Cohen
Check Point

Bio:

Itay Cohen (a.k.a. Megabeets) is the Head of Research at Check Point Research. Itay has vast experience in malware reverse engineering and other security-related topics. He is the author of a security blog focused on making advanced security topics accessible for free. Itay is a maintainer of the open-source reverse engineering frameworks Rizin and Cutter. In his free time, he loves to participate in CTF competitions and contribute to open-source projects.

Israel Gubi
Check Point

Bio:

Israel Gubi is a security researcher and reverse engineer in the Malware Research Team at Check Point Research. Israel joined Check Point in 2017 and was part of the first cycle of the Check Point Security Academy. Israel mainly focuses on malware analysis and malware hunting of both cybercrime and Advanced Persistent Threat campaigns. In his free time, Israel loves any kind of sports, especially tennis and bouldering.

LAZARUS DECLARES WAR ON WINDOWS SYSTEM MONITORING

Abstract:

The Lazarus Group is one of the most active advanced threat actors and therefore also heavily tracked by cyber threat hunters. There are usually many malicious tools deployed to compromise endpoints in networks targeted by the group and their high activity triggers various Windows system events. This vast volume of samples and artifacts provides an advantage for the defenders, namely a higher chance of identifying the on-going compromise and plentiful evidence for digital forensics in a post-mortem investigation.

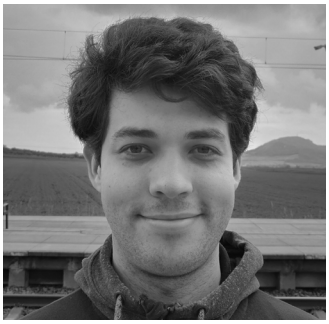
Since late 2021, developers from the Lazarus Group have started to implement a new malware that would be able to turn off as many Windows monitoring features as possible, effectively blinding most monitoring tools, security solutions and event logging. To achieve the desired functionality, they have created a user-mode module that gains write access to kernel memory using the CVE-2021-21551 vulnerability in a legitimate, signed Dell driver (the so called Bring Your Own Vulnerable Driver technique). Its current version contains eight distinct mechanisms targeting important kernel variables, functions, and structures. The module supports a wide range of operating system versions ranging from Windows 7.1 up to Windows 11 build 22500 and is actively being used in recent in-the-wild attacks.

In our presentation, we will focus on the most recent version of this malicious module discovered in summer 2022 containing newly added blinding features. We demonstrate how these mechanisms operate and what changes they make to the system once the module is executed. This involves monitoring of processes, images and threads; Windows registry; file system; Windows Filtering Platform services; Windows event tracing; and Prefetch files. The affected software includes EDRs/XDRs, firewalls, antivirus/antimalware products, digital forensics software etc. When compared to other APTs using BYOVD, this Lazarus case is unique, as it possesses a complex bundle of ways to disable monitoring interfaces that have never before been seen in the wild. For developers of security products, this can be an impulse for reevaluation of their implementations and increasing their solution's self-protection.

Peter Kálnai
ESET

Bio:

Peter Kálnai is a senior malware researcher at ESET. As a speaker, he has represented ESET at various international conferences including Virus Bulletin, AVAR and CARO Workshop. He earned his Ph.D. in mathematics at Charles University in Prague in 2020. In his free time he enjoys foosball and travelling.



Matěj Havránek
ESET

Bio:

Matěj Havránek is a malware analyst at ESET. In addition to malware research, he focuses on botnet activity tracking and developing analytic tools. He is a fan of ciphers, cryptography and enjoys challenges. In his free time he plays music, enjoys toying around with old hardware, online games and travelling.

HITCHING A RIDE WITH MUSTANG PANDA

Abstract:

Early this year, we stumbled upon a distribution server connected to security incidents affecting various institutions in Myanmar. A brief investigation revealed that the server was used for multiple attacks across the country, as well as a transition point for exfiltrated data.

Further inspection of the exfiltrated data revealed many high-profile government victims including police, army, and the Office of the State Administrative Council. Various political NGOs and the government opposition, including Karenni Nationalities Defense Force (the armed wing of the exile government), were also among the victims. Many sensitive documents were found on the server, for instance documents from the Office of the Chief Myanmar Air Defense Force with a list of staff along with their salaries, photo IDs, and family details. Gigabytes of data were exfiltrated on a daily basis, hinting at a large-scale operation. The Ministry of Immigration and Population was also breached, and thus passport scans from visa applicants, including diplomats, from various countries such as China, USA, and Great Britain were found.

The distribution server contained dozens of archives with various toolsets, some of them novel, while others were previously described and linked to the Mustang Panda group. The toolsets could be grouped into two groups: The first typically contained Korplug or other custom remote access tools. These were often accompanied by an USB launcher written in Delphi that has been previously associated with LuminousMoth. The second contained single-purpose tools that were selectively used against the targets.

Surprisingly, the group's operational security was also rather poor, allowing us to map the operation, track the development while resisting attempts to shake us off. This, together with the indiscriminate targeting and the tremendous scale of the operation with an impact on both civilians and diplomats around the world, makes an interesting case to study.

Adolf Středa
Avast

Bio:

Adolf Středa is a Malware Researcher at Avast. He specializes in botnets, more specifically botnet communication analysis and information extraction. He is also a PhD student at the Faculty of Mathematics and Physics of the Charles University in Prague, Czech Republic, specializing in cryptography. So far, he has presented his research at SantaCrypt, AVAR, Botconf, and Virus Bulletin.

Luigino Camastra
Avast

Bio:

Luigino Camastra is a malware researcher at Avast focused on reverse-engineering PE files, identifying malware families, and hunting advanced persistent threat groups. He holds a master degree in Computer Science from Czech Technical University in Prague. Luigino has presented his research at Virus Bulletin conferences, Avar, Botconf, MNSEC2020, and APWG. In his free time he enjoys playing futsal and CTF.

AOQIN DRAGON | NEWLY-DISCOVERED CHINESE-LINKED APT HAS BEEN QUIETLY SPYING ON ORGANIZATIONS FOR 10 YEARS

Abstract:

Executive Summary

- Aoqin Dragon, a threat actor SentinelLabs has been extensively tracking, has operated since 2013 targeting government, education, and telecommunication organizations primarily in Southeast Asia and Australia
- Aoqin Dragon seeks initial access primarily through document exploits and the use of fake removable devices
- Other techniques the attacker has been observed using include DLL hijacking, Themida-packed files, and DNS tunneling to evade post-compromise detection

Based on our analysis of the targets, infrastructure and malware structure of Aoqin Dragon campaigns, we assess with moderate confidence the threat actor is a small Chinese-speaking team with potential association to what Mandiant largely tracks as UNC94.

Overview

SentinelLabs has uncovered a cluster of activity beginning at least as far back as 2013 and continuing to the present day, primarily targeting organizations in Southeast Asia and Australia. We assess that the threat actor's primary focus is espionage and relates to targets in Australia, Cambodia, Hong Kong, Singapore, and Vietnam. We track this activity as 'Aoqin Dragon'. The threat actor has a history of using document lures with pornographic themes to infect users and makes heavy use of USB shortcut techniques to spread the malware and infect additional targets. Attacks attributable to Aoqin Dragon typically drop one of two backdoors, Mongall and a modified version of the open source Heyoka project.

Threat Actor Infection Chain

Throughout our analysis of Aoqin Dragon campaigns, we observed a clear evolution in their infection chain and TTPs. We divide their infection strategy into three parts.

1. Using a document exploit and tricking the user into opening a weaponized Word document to install a backdoor

2. Luring users into double-clicking a fake Anti-Virus to execute malware in the victim's host

3. Forging a fake removable device to lure users into opening the wrong folder and installing the malware successfully on their system. Initial Access via Exploitation of Old and Unpatched Vulnerabilities

During 2012 to 2015, Aoqin Dragon relied heavily on CVE-2012-0158 and CVE-2010-3333 to compromise their targets. In 2014, FireEye published a blog detailing related activity using lure documents themed around the disappearance of Malaysia Airlines Flight MH370 to conduct their attacks. Although those vulnerabilities are very old and were patched before being deployed by Aoqin Dragon, this kind of RTF-handling vulnerability decoy was very common in that period.

There are three interesting points that we discovered from these decoy documents. First, most decoy content is themed around targets who are interested in APAC political affairs. Second, the actors made use of lure documents themed to pornographic topics to entice the targets. Third, in many cases, the documents are not specific to one country but rather the entirety of Southeast Asia.

AOQIN DRAGON | NEWLY-DISCOVERED CHINESE-LINKED APT HAS BEEN QUIETLY SPYING ON ORGANIZATIONS FOR 10 YEARS

Joey Chen
SentinelOne

Bio:

Joey Chen is working as a Cyber Threat Researcher for SentinelOne Incorporated in Taiwan. His major areas of research include incident response, APT investigation, malware analysis and cryptography analysis. He has been a speaker at HITB, Virus Bulletin, CODEBLUE, DeepIntel, HITCON and CYBERSEC, etc. Now he is focusing on the security issues of target attack, emerging threats and IOT systems. He also develops an automation intelligence platform to help his team get more sleep at night.

CONTI LEAKS: BEHIND THE CURTAIN OF RANSOMWARE OPERATIONS

Abstract:

Conti Leaks - a dump of internal Conti ransomware gang conversations from the last two years offers an unprecedented insight into the inner workings of a multimillion-dollar cybercrime organization. In our talk, we first describe our approach to analyzing this massive data leak. Next, we will share insights into the operational side of the gang, such as organizational structure, HR, and nuances of offline and online collaboration. Finally, we will focus on Conti negotiation team's conversations and talk about the business side of ransomware operation, such as their processes in defining extortion demands and techniques for negotiation with victims.

Michael Abramzon
Check Point

Bio:

Michael Abramzon is a Technology Leader and a former Team Leader in the Threat Intelligence group of Check Point Research. For the last seven years, Michael has been involved in various research fields, from analyzing large-scale campaigns and APT groups, to developing open-source tools such as Vba2Graph.

Sergey Shykevich
Check Point

Bio:

Sergey leads the Threat Intelligence Group of Check Point, which monitors, analyzes and researches cyber threats around the world.

Prior to joining Check Point, Sergey led cyber threat intelligence and cyber defense teams in the elite Unit 8200 of the Israeli Intelligence Forces. More recently, Sergey led the threat intelligence and the research in Q6 Cyber, US based cybercrime intelligence company.

Sergey is a frequent speaker on different industry conferences, including DCC, Underground Economy, BSides, FraudCON, etc.

CRAWLECTOR: A THREAT HUNTING FRAMEWORK

Abstract:

Compromised websites can be used for drive-by-download attacks, water-hole attacks, social engineering, web skimming, ad injection, and hosting exploit kits. The volume of malicious traffic from such websites mandates an automated approach to finding threat intelligence quickly and efficiently. In this talk, we are presenting a new threat hunting framework called Crawlector (a combination of Crawler & Detector), signed for scanning websites for malicious objects, in a fully automated manner. Moreover, Crawlector supports online/offline scanning, spidering websites to discover additional links, Yara as a backend detection engine, digital certificate scanning, and querying URLhaus to find malicious URLs on the page, among others. The framework's operations are highly customizable. To demonstrate the framework's effectiveness and performance, we'll highlight some interesting results from scanning the top 700k Alexa websites and top 100k WordPress sites. Furthermore, this talk will additionally address the design processes and decisions made during the development of the framework.

Crawlector features include:

1. Supports spidering websites for finding additional links for scanning
2. Integrates Yara as a backend engine for rule scanning
3. Supports online and offline scanning
4. Supports crawling for domains/sites digital certificate
5. Supports querying URLhaus for finding malicious URLs on the page
6. Supports querying the rating and category of every URL
7. TLSH
8. JARM Hash
9. Supports expanding on a given site, by attempting to find all available TLDs and/or subdomains for the same domain
10. This feature along with the rating and categorization, provides the capability to find scam/phishing/malicious domains for the original domain
11. Saves scanned websites pages for later scanning (can be saved as a zip compressed)
12. The entirety of the framework's settings are controlled via a single customizable configuration file
13. All scanning sessions are saved into a well-structured CSV file with a plethora of information about the website being scanned, in addition to information about the Yara rules that have triggered
14. One executable
15. Written in C++
16. The framework and a transpiler that converts EKFiddle rules to Yara rules will be released on GitHub after the talk

CRAWLECTOR: A THREAT HUNTING FRAMEWORK

Mohamad Mokbel
Trend Micro

Bio:

Mohamad Mokbel is a senior security researcher at Trend Micro. He's responsible for reverse engineering vulnerabilities and malware C&C communication protocols, among others, to write custom filters for TippingPoint NGIPS. Before joining Trend Micro, Mohamad worked for CIBC in the SoC, one of the top five banks in Canada as a senior information security consultant - investigator (L3) where he realized that experience in the operation field is extremely important to understanding the real sides of offence and defense. Before CIBC, Mohamad worked for TELUS Security Lab as a reverse engineer/malware researcher for about 5 years. He's been doing reverse code engineering for the last 14 years. His research interests lie in the areas of reverse code engineering, malware research, intrusion detection/prevention systems, C++, compiler and software performance analysis, and exotic communication protocols. Mohamad holds an MSc. in Computer Science from the University of Windsor.

BEERS WITH TALOS

Podcast

THREATS, BEERS & NO SILVER BULLETS

Join Lurene, Matt, and Mitch from Talos
(and their guests) to talk about emerging threats,
hacking all the things, and vital security topics.

Caution: *You can accidentally learn things while enjoying this podcast.*

Listen at **cs.co/bwt**

BEHIND THE MIRRORFACE MASK: LODEINFO MALWARE INTERFERING WITH JAPANESE ELECTIONS

Abstract:

In the weeks leading up to the Japanese House of Councillors election in July 2022, the APT group that ESET researchers track as MirrorFace launched a spearphishing campaign against Japanese political entities. Impersonating the Liberal Democratic Party's PR department, the malicious actors prompted email recipients – among them party members – to spread attached videos on social media on behalf of Fumio Kishida, the party's president. Not recognizing the malicious nature of the attachments, which were actually Windows executables, some recipients even unintentionally helped the threat actor to spread the emails by forwarding them to other party members. Once the email attachment was opened, LODEINFO malware – in use since 2019 and exclusively against Japanese entities – was executed, opening the door for the threat actor to move to the next stage of the attack.

In our presentation, we will introduce the audience to the MirrorFace APT group, a threat actor exclusively targeting Japanese entities with the LODEINFO malware. Then, we will move on to a detailed description of the campaign against Japanese political entities. In the process, we will unearth MirrorFace tactics and procedures that haven't been published in detail before. We will close up the presentation by describing the evolution of the LODEINFO malware over the past few years by pointing out the changes in the malware's capabilities.

Dominik Breitenbacher
ESET

Bio:

Dominik is a malware researcher at ESET. Coming from academia, Dominik joined ESET in 2019 to track activities of APT groups. In particular, Dominik tracks Kimsuky, Operation In(ter)ception and MirrorFace. In his spare time, Dominik plays video games and watches bad movies.

MAIMLA: MAKE ARTIFICIAL INTELLIGENCE MACHINE LEARNING AGAIN

Abstract:

Although machine learning has been transforming the cybersecurity industry for decades, many people only start paying attention when buzzwords such as "artificial intelligence" enter the conversation. With the arrival of nextgen vendors, the technology itself was buried under layers of "silver bullet" marketing, obscuring its true contribution to threat detection. In our talk, we'll try to cut through the noise and show how we've been deploying machine learning since the 1990s and how it has become a key component of our multilayered architecture. As a reality check, we will demonstrate how natural language processing methods (transformers) can help mitigate one of the admin's worst nightmares – a destructive ransomware attack. For more context, we'll venture into how adversaries use genetic and automation algorithms to create new variants of their malicious products. In the final section of our talk, we will describe potential threats that might leverage machine-learning technology in the foreseeable future.

Filip Mazan
ESET

Bio:

Filip Mazán is a Senior Software Engineer and Team Lead at ESET. He joined ESET as a malware analyst in 2013, then switched to a software engineering role, and since 2019 has been leading a team responsible for automated threat detection and application of artificial intelligence in threat hunting. Some of the highlights of his career include speaking at the RSA Conference and membership in several botnet eradication groups taking on botnets such as Dorkbot and Gamarue. Currently, he is working on various machine-learning research projects leveraging deep learning. In his free time, Filip likes cooking, gardening and tinkering with home automation projects.

USING AI/ML TO BUILD EFFECTIVE DATA SECURITY PROGRAMS

Abstract:

It's time to break down the barriers between data and cybersecurity professionals. In this session, Ronan Murphy will discuss how to unify these roles into one shared goal of protecting your data the—21st century currency of business.

Ronan has worked at the cold face of the cybersecurity industry for the last 20 years, and his companies are responsible for protecting some of the world's leading organisations. The presentation will include an analysis of the circumstances that led to one of Europe's most high-profile Ransomware attacks during the Covid Pandemic and the subsequent fall-out.

This case study will form the basis of the presentation to understand how organisations can implement a Zero Trust Strategy on their data that will ultimately help improve their Cybersecurity Strategy.

Ronan Murphy
Getvisibility

Bio:

Ronan is an accomplished executive with over 20 years of experience in the tech industry. Ronan is the Founder of Getvisibility, an AI-based data security company delivering cutting-edge data security solutions, & founder and executive chairman of Smarttech247 plc, a global multi-award-winning managed cybersecurity company.

STORY OF NEW ATTACK FRAMEWORK

Abstract:

Attack frameworks are becoming prevalent across the threat landscape. Adversarial frameworks consist of a command and control tool and the custom Remote Administration Tools which can be employed by various threat actors in their campaigns. As defenders, it is important to keep track of offensive frameworks so that enterprises can effectively defend against attacks employing these tools.

In this presentation, I will talk about the Cisco Talos discovery of new attack frameworks known as Manjusaka and Alchimist in the wild which consist of command and control tools and Remote Administration Tools that contain all the features one would expect from an implant. These tools are written in the most modern and portable programming languages to target Windows, Mac OS X and more exotic flavors of Linux operating systems. The fact that the developer made a fully functional version of the C2 available would increase the chances of wider adoption of this framework by malicious actors.

Chetan Raghuprasad
Cisco Talos

Bio:

Chetan Raghuprasad is a Research Engineer with the Cisco Talos Intelligence Group, focusing on threat hunting of latest threats and threat campaigns in the threat landscape, reversing malwares to uncover its TTPs to identify actor's intention, attributing them to specific actors. Chetan also represents Cisco Talos publicly by publishing his research in Talos blogs and speaking at the IT conferences in the world. Chetan Raghuprasad has 13 years of experience in the Information Security sector, having worked within cyber incident response, Digital forensics, Cyber threat research at Financial institutions, Consulting and Technology companies.

WIN-P9NRMH5G6M8" - TRANSPARENT TRIBE PERUSSIAN

Abstract:

In 2022, Pakistan-based Transparent Tribe, AKA APT36, has broadened its horizons and adopted new TTPs. Since 2016, when this APT group targeted the Indian Embassy in Riyadh, Saudi Arabia, it has repeatedly targeted official Indian institutions, including baiting Indian Defence personnel. However, now, this group has begun to target sectors other than Central Government and Defence. Recent targets have included the State Government of West Bengal (India) and the Indian Institute of Technology, Hyderabad (an educational institution). In addition to these, there have also been campaigns against Indian IT firms, where the usual infection vectors, weaponized Office documents, masquerade as candidate resumes.

Our deeper investigations into recent Transparent Tribe campaigns revealed an interesting new TTP common to all of them; the outsourcing of hosted C2s. We found an open RDP port in one C2 IP used by Transparent Tribe with a self-signed SSL certificate bearing Common Name "WIN-P9NRMH5G6M8".

We pivoted on this Common Name (CN), expecting but a handful of hits. In reality, however, we ended up drowning in a deluge of tens of thousands of IPs, with exposed RDP, each using different SSL certificates with the same CN. These IPs were associated with ISPs in different geolocales; several of them have been involved in other common cyber-attacks, ranging from hosting phishing sites to hosting a flavour of the Log4Shell exploit (CVE-2021-44228) in June of 2022. Surely, not all of these can belong to the Transparent Tribe actors. What's more probable is that this unique CN is associated with an outsourced service. We had to dig deeper.

We discovered that this Virtual Private Service is being sold in a Telegram group bearing the username, surprise, surprise, "WIN-P9NRMH5G6M8". Further pivoting revealed this to be a premium bullet-proof-hosting-services option offered by an actor or group who lists both Persian and Russian in the language profile of its Russian social media page. We were also able to track down a video website (Iranian YouTube-like) associated with this actor. The plot thickens. What could have been the reason for Transparent Tribe to be linked to these characters?

In this presentation, we examine the latest Kill Chain employed by Transparent Tribe, with particular focus on changes incorporated in 2022, and the possible reasons for these. We will also reveal detailed identifiers associated with the threat actors behind the infrastructure used by Transparent Tribe with a view to gauge the extent of the relationship, and whether the same or similar infrastructure is or might be used by other APT actors too.

Arun Kumar Shunmuga Sundaram
K7 Computing

Bio:

Arun Kumar Shunmuga Sundaram, a Computer Science Master's graduate from the University of Glasgow, has been working as a Threat Intel Team Lead at K7 Threat Control Labs for the past 8 years. He works on curating and optimizing the Threat Intel feed and monitoring various threat actors. His research findings have also contributed to the K7 lab blog. Apart from being passionate about reversing, he is an avid gamer and loves to follow up on indie gaming.

Rajeshkumar R
K7 Computing

Bio:

Rajeshkumar R is a Threat Researcher at K7 Threat Control Labs and holds a Master's degree in Computer Applications from Anna University, Chennai. His core responsibilities include reversing and providing detection at multiple layers for prevalent malware in addition to monitoring the latest trends in ransomware attacks. He also publishes his research findings on the K7 lab blog from time to time. Outside of malware research, he likes to spend his spare time swimming and has a keen interest in current events and politics.

INSECURE SECURITY UPDATE : LAUNCHING COUNTER ATTACKS WITH CYBER AWARENESS CAMPAIGNS MAGNIBER RANSOMWARE NEW DELIVERY TECHNIQUE

Abstract:

The continuous pursuit of improving and innovation across every aspect of human life can be seen and proven that even threat actors search for a newer way to distribute their crafts. Magniber Ransomware is one of the malware families that was seen evolving every now and then. It was first seen in 2017 that used Magnitude Exploit Kit as a delivering platform, that often used by other ransomware families such as Cerber, Locky and Cryptowall.

Fast forward to this year, 2022, Magniber Ransomware has been seen lurking around again but this time, it chose to have a different entrance.

Nowadays, cyber security professionals are raising security awareness, campaigning and urging people to regularly update their software so that they can lower the risk of being exposed and attacked caused by leveraging known vulnerabilities of outdated systems. Now here comes a Windows Update that should be good in all aspect, however unbeknownst to most, malicious actor crafted a Fake Windows Update and bundled it with Magniber Ransomware. Although this is not the first of fake application being used to deliver malicious content, this is the first for a ransomware to have MSI as the chosen gate for attack.

This research focuses on the new attack vector used by Magniber Ransomware. Unveiling how malware actors was able to use MSI as a package for Magniber ransomware by leveraging a MSI feature coupled with a malicious component. This research will also showcase a tool known as Orca, a Microsoft database table editor that can be used to understand how Magniber was executed without being noticed. Furthermore, this research will also explore how can MSI be used in other ways as a distribution technique. Finally, seeing Magniber pioneered a new distribution technique for ransomwares, this research will also explore and monitor if other ransomware families will follow its steps. As the approach of finding new ways to attack and enter the environment evolves, the need to update our current cyber awareness campaigns to secure and strengthen our gates is a way to counter this attack.

John Karlo De Mesa Agon
G DATA

Bio:

Karlo has been in the Threat Analysis and Reverse Engineering area of Information Security for almost 8 years. His experience in creating pro-active detections through correlation of file metadata was critical in identifying malwares and even prevented an outbreak of ransomware. Coupling these technical skills, with fun and outgoing character, he not only works well with the team but he guides them in working out solutions as a seasoned Virus Analyst. He enjoys watching movies and anime with his wife and has recently been blessed with to be father to a healthy baby boy.

Lovely Jovellee Lyn Bruiz Antonio
G DATA

Bio:

With more than 9 years in the Information Security Industry, Lovely's experience includes research, analysis and creating detection and remediation signatures for malicious software. She is also well-versed in website analysis for false positive checking and blocking. Lovely has been part of malware research projects and has been fortunate to have presented to previous AVAR conference. She recently got married to another virus researcher and is looking forward to building a family of her own.

SECURITY-REDUCING APPS: A CALL TO ACTION

Abstract:

As AVs get better operationalized in their fight against unwanted software (UwS), their combined pressure is driving the software monetization industry toward finding the gaps in AV policies so they can continue to exploit consumers for easy money. The big gap in AV policies these days, unfortunately, is around apps that make their computers more vulnerable to attacks. The result? A proliferation of apps that needlessly reduce their customers' security postures and set them up for future attacks. Examples of these apps include VPNs that install self-signed trusted root certificates and free apps that monetize by installing proxies that share their internet connection and processor. Lately these security-reducing apps are grabbing public attention: articles about them are popping up in both security blogs and computer industry news. Some platforms and AVs are beginning to respond – they detect after others have called them out. But the platforms and AVs have been slow to update their policies, and slow to detect these apps as UwS, which leaves a gap that software monetizers continue to exploit. Our session will show examples of how these apps reduce their customers' security postures. We will highlight the platform and AV public policy gaps that have led to the spread of them. We'll make suggestions as to how AVs can enhance their policies to better protect their customers from these apps.

Hong Jia
AppEsteem

Bio:

Hong Jia is chief Research Officer at AppEsteem Corp. She leads application certification review and deceptor application hunting teams. She worked for fifteen years at Microsoft, where she led the antimalware research labs in the US, Canada, and China and drove the relationships between Microsoft's antimalware teams and the China security companies. She is also one of the founders of ThreatBook Labs, where she ran research and response teams.

Dennis Batchelder
AppEsteem

Bio:

Dennis Batchelder is the President of AppEsteem Corporation, where he's eradicating unwanted software while helping the software monetization industry thrive. He spent eight years at Microsoft, where he led their antimalware efforts to protect billions of customers through real-time antimalware products and services, industry partnerships, and continuous analysis of threat intelligence using machine learning and the cloud. Prior to Microsoft, Dennis owned the threat and security information management product lines as a Senior Vice President at Computer Associates, which he joined after founding, running, and selling them a network security product company. Dennis has worked for more than thirty years in the security industry holding various leadership roles in the US and India. He lives in Seattle, Washington. Dennis is the author of the Soul Identity series of techno-thriller novels.

FROM RED TO BLACK AND BEYOND - EVOLUTION OF A RANSOMWARE STRAIN

Abstract:

A new ransomware family called EpsilonRed made its debut just before last summer. It relied on a set of different PowerShell scripts for distribution, which, at the time, was becoming a more common way for ransomware affiliates to deploy ransomware into corporate environments. Apart from being written in the Go programming language, EpsilonRed showcased some unique attributes and seemed to disappear just as quickly as it came; no one reportedly saw it after the first confirmed attack.

In this talk we will present how different ransomware families – such as EpsilonRed, BlackCocaine, and more - share the very same roots on the binary level, we'll discuss which current obfuscation techniques they utilize, and show how they've started to develop a method of combining C and Golang together to make analysis even more challenging. New ransomware strains appearing on the scene, doing their fair share of infection rounds, then quickly fading away was nothing new last year. The renewed interest shown by law enforcement agencies and some fruitful efforts resulting in raids, often made affiliates and creators of ransomware reconsider their actions. Officially, they seized operations, except often they really did not.

In this presentation, we will demonstrate how certain ransomware families are almost a one-to-one copy or a 'rebrand' of another existing family, their recent evolution involving obfuscation and anti-analysis techniques, and some recent development approach that involves the combination of Golang and C.

Robert Neumann
Acronis

Bio:

Robert Neumann is the head of the Cyber Protection Operations Center at Acronis. Besides managing teams to counterbalance the fight against cybercriminals, he is focusing on various short and long-term research projects, ranging from small scale malicious campaigns through niche malware and file formats to in-depth investigations and threat actor attribution.

Robert is a long-time security researcher, working in IT - and especially in IT security - for most of his career. His previous experiences at companies such as Virusbuster, Sophos and Forcepoint enabled him to understand and respond to cybersecurity challenges on different levels.

FROM RED TO BLACK AND BEYOND - EVOLUTION OF A RANSOMWARE STRAIN

Albert Zsigovits
Acronis

Bio:

Albert joins Acronis from a traditional, security blue-team background, kickstarting his cyber-career analyzing security events as a SOC IDS/SIEM Analyst, and later investigating cybercrime activity and data breaches as a Senior Incident Responder in a Fortune 50 company's internal CERT.

Following this, he joined a respected anti-virus company to set his foot in malware analysis and reverse engineering.

His specialties include cyber threat hunting, memory forensics, and signature development.

He enjoys the challenge of connecting the dots between cybercrime and criminal rings leveraging threat intelligence and open-source intelligence techniques.

He is very keen on publishing malware analysis reports and takes pleasure in publishing educative content on malware.

Albert is also a former conference speaker at BSidesVienna, DisobeyFi, Hacktivity, SEC-T, and VirusBulletin.

YOU HAVE TO SEE IT TO DISRUPT IT: MAPPING THE CYBER CRIMINAL ECOSYSTEM

Abstract:

Cybercrime has become professionalized, diversified, and integrated over the past decade. This evolution has resulted in a much more complex, expansive criminal landscape, further challenging the ability of the cybersecurity industry and law enforcement to counter it. If we want to disrupt these criminal operations, we need to understand this ecosystem more fully, know how the various parts link together, and maintain that insight dynamically overtime. This talk will describe a project designed to provide such views of the criminal ecosystem. Called the Cybercrime Atlas, this joint effort by multiple organizations, including the Cyber Threat Alliance, will enable the cybersecurity industry, civil society, the financial sector, and governments to see the criminal ecosystem from different viewpoints and to take effective action to disrupt it.

Michael Daniel
Cyber Threat Alliance

Bio:

Michael Daniel serves as the President & CEO of the Cyber Threat Alliance (CTA), a not-for-profit that enables cyber threat information sharing among cybersecurity organizations. Prior to CTA, Michael served for four years as US Cybersecurity Coordinator, leading US cybersecurity policy development, facilitating US government partnerships with the private sector and other nations, and coordinating significant incident response activities. From 1995 to 2012, Michael worked for the Office of Management and Budget, overseeing funding for the U.S. Intelligence Community. Michael also works with the Aspen Cybersecurity Group, the World Economic Forum's Partnership Against Cybercrime, and other organizations improving cybersecurity in the digital ecosystem. In his spare time, he enjoys running and martial arts.

STREAMLINING THREAT DETECTIONS BY OPERATIONALIZING SIGMA INTO SIEM/ MITRE CAR DETECTIONS AUTOMATICALLY

Abstract:

Streamlining Community Sourced Threat Detections by Operationalizing Sigma into SIEM Detections Automatically Submission Orientation: Defensive Security Live Demos: Yes. We would like to demonstrate how our tool can automatically convert sigma detections into SIEM queries. In this demonstration, we would like to take a sigma file which we have pre-emptively created and convert it into an SIEM query via our tool. We would then like to take the SIEM query generated and run it on the target SIEM to check for matches. We would also like to showcase the AWS Lambda implementation of the above tool, which allows one to run the tool as an API endpoint, allowing seamless integrations with other security technology verticals such as SOAR etc.

While there are different SIEMs being used by different organizations, knowledge transfer has become difficult for organizations sharing detections for the same type of attacks. To solve this, sigma was introduced which allowed one to share the detection without having to bind it to a query language. But SIEMs today are not able to readily ingest Sigma detections as search queries but rather require a custom search query Eg: Lucene, Splunk search processing language, Devo LINQ etc. In this talk, we show our research where we have been able to engineer a tool to convert Sigma queries to SIEMs and a methodology to streamline detections across community sourced detections into actionable SIEM queries.

Aashiq Ramachandran
Cyware Labs

Bio:

I enjoy designing and automating security processes, building solutions that add visibility into processes and research and development ensuring we add human effort where it's most needed.
I am passionate about furthering cybersecurity and contributing to open-source cybersecurity projects. I strongly believe automation and orchestration of security is foundational to combat cybersecurity threats.

SUMMARY OF LINUX KERNEL SECURITY PROTECTIONS AND ATTACK

Abstract:

Linux kernel goes through very rapid changes each release. Over each release new protections and mitigations are added to make it more secure against different category of attacks. Unlike other platform, Linux security features are not advertise enough and most of the time limit to a mail thread. Since Linux is getting popular day by day in different sectors of industries, it is important for a researcher or an administrator to be aware about what protection it provide against sophisticated attacks targeting Linux kernel. In this session, I will take you through the different security features that Linux kernel has introduced over years and their limitations or bypasses. We will go though few demos to verify the working and bypasses of these protections. In the end I will discuss what is missing on Linux kernel that can be improved in future. This talk will help security researcher in identify the current Linux security protection and gaps presents in Linux kernel. With this knowledge they can tweak their product, for example an AV vendor working on Linux security need to be aware what protection is already present before working on something new. A developer dealing with Linux kernel development can also utilize this session to identify the security issues there code may hold and things they need to take care and ignore to make their modules or components secure.

Shubham Dubey
Microsoft

Bio:

Shubham is a Security Researcher 2 at Microsoft where he works for Microsoft's Defender product. His expertise lies in low level security and internals which includes reverse engineering, exploitation and firmware security. Prior to joining Microsoft, Shubham was Security researcher at Antivirus company working in exploit prevention team where he contributed to protect customers from 0-days and vulnerabilities in the wild. Shubham has worked on multiple independent project on kernel level and firmware security. He owns a security blog nixhacker.com where you will find lots of content on low level security and internals.

LAZARUS AND THE TALE OF THE THREE RATS

Abstract:

The Lazarus APT has been targeting the renewable energy sector across Japan, United States and Canada. On these campaigns it has used some old tools, but more importantly it has used a new RAT built from scratch. This new RAT is based on QtFramework, a graphical interface which has no record of being used to build malware before. In this presentation Vitor will take a deep dive into this new RAT and will show the techniques, tools and procedures used by Lazarus APT to compromise the organizations, on this highly targeted campaign.

Vitor Ventura
Cisco Talos

Bio:

Vitor Ventura is a Cisco Talos security researcher and manager of the EMEA and Asia Outreach team. As a researcher, he investigated and published various articles on emerging threats. Most of the day Vitor is hunting for threats, reversing them but also looking for the geopolitical and/or economic context that better suits them. Vitor has spoken in conferences, like LabsCon, VirusBulletin, NorthSec, Recon, Recon Bruxels, Defcon's Crypto and Privacy Village, among others. Prior to that he was IBM X-Force IRIS European manager and lead incident responder, and at IBM X-Force RED where he was a lead penetration tester. Vitor holds a BSc in Computer Science and multiple security related certifications like GREM (GIAC Reverse Engineer Malware), CISM (Certified Information Security Manager).

THREAT HUNTING IN M365 ENVIRONMENT

Abstract:

Over the last few years, Threat Actors have augmented their efforts in developing novel and sophisticated attack techniques to target Enterprise Cloud environments. Microsoft 365 is a cloud based software as a service provided by Microsoft and includes services like Exchange online, Flows, SharePoint online, Teams. Attackers consistently target M365 services in order to gain initial access, maintain persistence and perform data exfiltration. Several investigations have revealed that threat actors have not only been able to successfully compromise Cloud environments but also persist and move laterally. Organizations have found it increasingly difficult to protect Cloud services and detect threat actor activities. We will talk through ways of how blue teams can hunt for some of the techniques that threat actors use to target M365. Some of the areas that we will cover include

1. Automated Email Forwarding
2. Delegation
3. Mailbox folder Permissions
4. OAuth Grants
5. Flows to automate Data Extraction
6. MFA Bypass Scenarios
7. Persistent Privileged roles
8. Abusing SharePoint Online
9. Log evasion techniques
10. Hunting from Unified Audit Logs

Thirumalai Natarajan
Mandiant

Bio:

Thirumalai Natarajan is a Senior Manager with Mandiant Consulting where he leads incident response remediation engagements for large-scale breaches and proactive security assessments for global organizations. Over his career experience, Thiru has built and managed security operation centers and detection engineering teams across APAC to support organizations to improve their detection and defense posture. He has advisory experience with CXO's and senior management across industries during the time of compromise. He has spoken in various conferences such as Black Hat Asia, Virus Bulletin, BSides SG, SANS Threat Hunting, DFIR summits.

THREAT HUNTING OF CRIMSONRAT FROM APT36/ TRANSPARENT TRIBE GROUP

Abstract:

As part of my research among new malware and widespread active vulnerabilities it was interesting to work on actives of Crimson RAT which was active and prominent in some countries in Asian region.

This trojan was actively used by APT36 (aka Transparent Tribe) among some other tools. The malware/group was targeting various government entities as well as high profile educational institutes like IITs, that made it more interesting to conduct a deep dive in this RAT.

This presentation will cover various aspects about CrimsonRAT Malware Analysis & Threat Hunting.

- Types of issues faced during the Reverse Engineering of the malware
- Points like basic analysis, issues with sandbox executions, sandbox evasion capabilities, persistence methods
- Type of payloads and different secondary payloads analysis, behavioural indicators, threat hunting process
- How threat hunting queries are created
- How threat hunting output is further used and prevention against the malware

Amey Gat
Fortinet

Bio:

- Currently working as a Threat Researcher by Day 😊 Working from 17+ years in industry, previously worked as Threat Intelligence Researcher, Information Security consultant, Developer of Firewall/IDS/ IPS devices
- Worked in various aspects of Threat Intelligence like Darknet coverage, OSINT, Building & deploying Honeypots, Automation of Darknet data collection
- Moderator and Core Team member of hackers group www.Garage4Hackers.com, one of the leet hacker groups of India
- Python programmer, official programmer in the past and Now for automation and fun and the love of python
- Lock picking enthusiastic, done lock picking workshop at Garage4Hackers meet. Also conducted the first Lock picking workshop in India at NullCon 2015
- Hardware and Electronics enthusiastic, works with AVR and other embedded devices as a hobby. Created first ever hardware badge of Nullcon conference in 2014

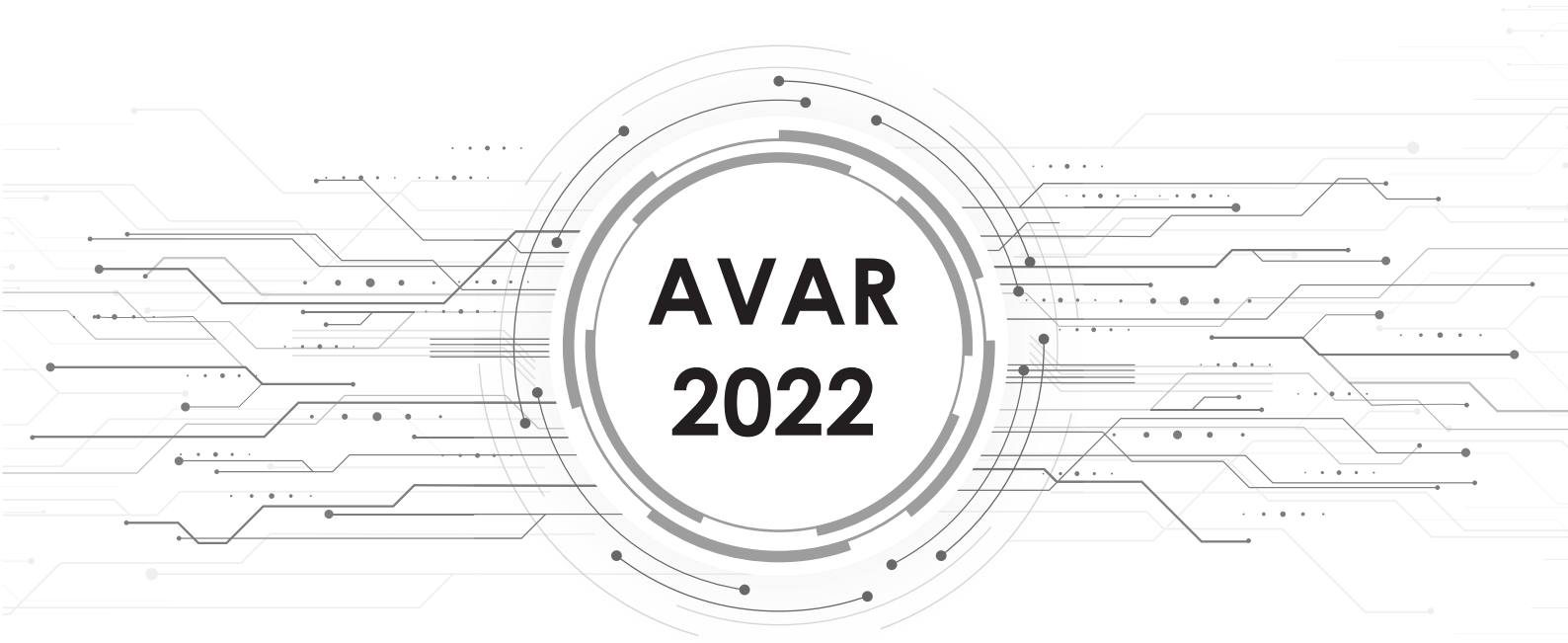
Dear friends and acquaintances, dear family and colleagues,

Since 1994, RED NOSES Clowndoctors have been bringing laughter where it may not be suspected but is desperately needed: Too little patients on wards in paediatric surgery, cardiology and oncology and intensive care units, to children and young people in special and curative education institutions and also to adults and senior citizens in care and rehabilitation centres. Every amount helps. Scan the QR code to access the donation website.

RED NOSES CLOWNDOCTORS International

supported by:

AV comparatives



RESERVE PAPER

IF THE HYPE DOESN'T KILL YOU, FLAWED OR MISSING ANALYSIS WILL

Abstract:

Many vendors like to use dazzling terms that describe the same technology their competitors have and/or are doing the same thing that their competitors do. As an analogy, one company that sells bottled water calls theirs pure while another says purified. The one that wants to dazzle with science will talk about how "we've combined 2 sets of hydrogen atoms with one oxygen molecule having the specific atomic weight of 8 in order to create the purest water that is scientifically attainable. Or, my favorite, "Now with twice as much hydrogen as oxygen." The last one actually was on a billboard, albeit deliberately humorous.

When testing security products, the quality of the hype doesn't cut it. The quality of protection is king. But deciding on a solution requires more than beautiful numbers. If one product protects against 100% of the attacks against it, while another scores 94%. Which product is best? What about the ones scoring better or worse than 94%? The answer is that you don't have enough data to reach a logical decision. For example, in some cases regulatory compliance requirements must prioritized. If a product must be "accredited" as providing PCI DSS requirements, then non-accredited products are not viable solutions, regardless of quality. There are a variety of considerations that must be evaluated alone and in conjunction with each other. In this presentation we will provide anti-hype information designed to help IT practitioners improve the quality and comprehensiveness of their analysis of the results of security product test data, regardless of what test organization is providing results. Data doesn't lie, but numbers laugh at those who make purchase decisions based on data without analysis.

Randy Abrams
SecureIQLab

Bio:

Randy Abrams is a 25+ veteran of the cyber security industry. During his 12-year career at Microsoft Randy designed, implemented, and managed the multiscanning system used by Microsoft to ensure that infected software is not released, and worked as the Operations Manager for the Global Infrastructure Alliance for Internet Security, a program that provided security information to ISPs across the globe. Randy has also served as the Director of Technical Education at ESET, a Research Director at NSS Labs, a Senior Security Analyst at Webroot, a senior security analyst at OPSWAT, and is currently a senior security analyst for cloud security company SecureIQLab. From 2000 to 2019 Randy served on the board of directors for the Association of anti Virus Asia Researchers and remains on the education outreach advisory board for the organization.

K7 SECURITY

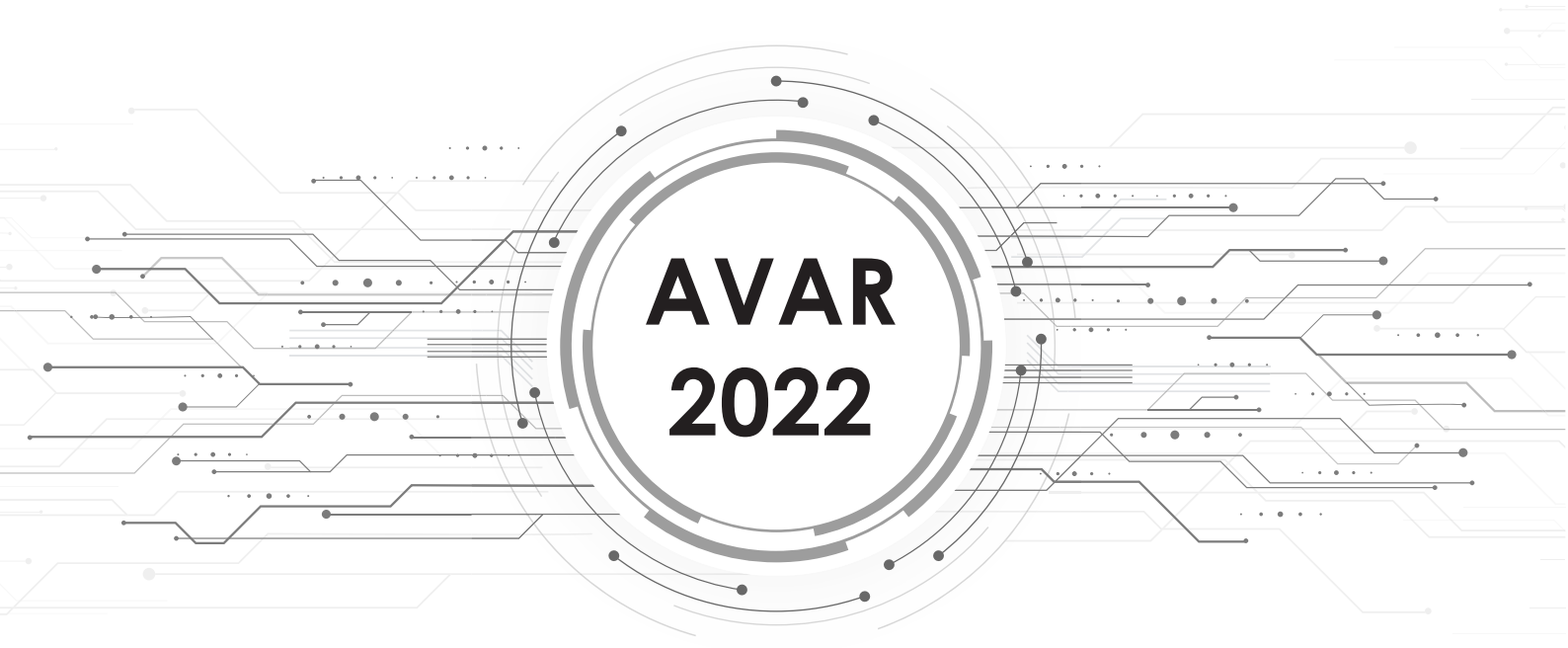
Boundaryless Cybersecurity
for the No-Perimeter Enterprise

International Award-Winning Cyber Protection for the

- 24/7, Always Connected
- Work-From-Anywhere Business

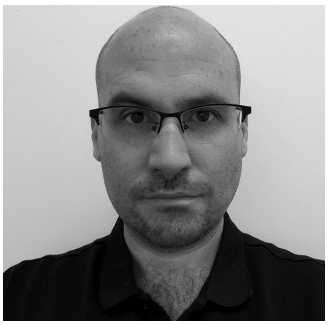
www.k7computing.com

India | USA | UAE | Singapore



PANEL MEMBERS

PANEL DISCUSSION – CYBERSECURITY TRENDS FOR 2023 AND BEYOND



Yul Bahat
Kiteworks

Bio:

Yul Bahat, CISSP, is a veteran Cyber Security specialist and evangelist, currently working as the Director of Cyber Security for Kiteworks, in charge of all product security aspects.

Previously, Mr. Bahat was the Senior Information Security Specialist at the Organisation for Economic Cooperation and Development (OECD), Head of Security Intelligence for the Israeli E-Gov agency, and Head of Information Security Audits for Aman, a leading Israeli consulting firm. He holds a BA in Computer Science from the Reichman University in Israel and an MBA from the International School of Management in France.

In addition to his regular professional activities, Mr. Bahat is considered an expert in his field, and has gave multiple presentations and keynote speeches in professional conferences, and has been interviewed as a subject-matter expert on multiple TV networks.

Ajay Kumar
CrowdStrike

Bio:

Ajay Kumar is the Regional Head- Cyber Security Services, Asia with CrowdStrike based in Singapore. Ajay heads Cyber Security and Risk Management Services portfolio and engages in cyber breach incidents and cyber security maturity initiatives and assessments across the industry as a trusted advisor.

Previously, he worked with Entrust as a Regional Managing Director-Asia Pacific in cyber security, identity and payment space. He also served as a Regional Marketing Director- APJ with Entrust and received "National Leaders in Marketing" award from CMO Asia Council and "Most Influential Technology Marketing Leaders" award from World Marketing Congress in 2016.

Earlier, Ajay worked in various Fintech, Financial Services and Banking organisations on senior positions and managed sales, business development and strategy functions.

Ajay is Singapore Chapter Anchor for Data Security Council of India (DSCI), a not-for-profit, industry body on cyber security and data protection, setup by NASSCOM® and committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and data privacy.

Ajay is a subject matter expert and speaker in payments, cyber security, enterprise technology and data privacy space and has about 22 years of experience in Asia Pacific and EMEA region.

PANEL DISCUSSION – CYBERSECURITY TRENDS FOR 2023 AND BEYOND

Anil Malekani
Microsoft

Bio:

Anil Malekani is Security Architect, Global Blackbelt for Microsoft Asia and based in Singapore. Anil has been working with various organizations across different industries including public-sector, helping them strengthen their security posture and modernize security operations for hybrid and multi-cloud environments.

Anil has been with Microsoft for over 12 years and has been part of the journey as the company expanded the security portfolio, enabling customers to do more with less, in the area of cybersecurity.

Rudy Lim
Accenture Security

Bio:

Equipped with more than 20 years of experience in Cyber Security, Rudy is currently leading the Data & AI Security and Platform Security practice for Accenture Security Southeast Asia. Through his past experience in Data Security, Endpoint Security, and Cyber Defense, Rudy gained a deeper understanding of the overall Cyber Security landscape and the challenges organizations are facing today. He is also a passionate developer, which allows him to study various attack techniques employed by threat actors.

PANEL DISCUSSION – CYBERSECURITY TRENDS FOR 2023 AND BEYOND

Steven Sim
ISACA SG Chapter

Bio:

Steven Sim has worked for more than 25 years in the cybersecurity field with large end-user enterprises and critical infrastructures, undertaken global CISO role, driven award-winning CSO50 security governance and management initiatives and headed incident response, security architecture, technology and operations at local, regional and global levels. He leads cybersecurity across PSA Group, heading 8 direct reports at Group Cybersecurity Department and indirect reports across regional offices and local business units in 42 countries.

Always keen to give back to the community, he also volunteers at the ISACA Singapore Chapter (which won ISACA Global Outstanding Chapter Achievement in 2022) in as the President (from 2021 to 2022) as well as at OT-ISAC (since 2021), the second key thrust of the Singapore's OT Cybersecurity Masterplan 2019, as the Chair of the Executive Committee, and holds a Masters in Computing, CCISO, CGEIT, CRISC, CISM, CISA, CDPSE, CISSP as well as technical certifications GICSP, GREM, GCIH and GPPA.

He is recognised as #1 CSO in the inaugural IDG's CSO30 ASEAN Awards 2021, as a winner in the ISACA Outstanding Chapter Leader Achievement Awards 2022, #7 in Global Cyber Security Thought Leaders under the IFSEC Global Top Influencers 2022, as a Global Cybersecurity Leader 2022 (CXOTV), an ISACA Global Outstanding Chapter Leader in 2022, in the Peerlyst 29 Highly Influential CISOs list, a Singapore SkillsFuture Fellow and a Professional (Leaders) Finalist in the inaugural Singapore's Cybersecurity Awards 2018.

PANEL DISCUSSION – THE CURSE OF THE FALSE POSITIVE

Stefan Haselwanter
AV-Comparatives

Bio:

Stefan Haselwanter graduated from the University of Innsbruck in Austria with a Bachelor degree in Computer Science. He has been working as a security tester and developer for AV-Comparatives since 2016. His main work focuses on testing and assessing protection capabilities as well as other security-related aspects and features of security software for different platforms, documenting findings, and writing test report. Besides that, he closely works together with the AV-C developer team to continuously improve the in-house testing frameworks and systems.

Robert Neumann
Acronis

Bio:

Robert Neumann is the head of the Cyber Protection Operations Center at Acronis. Besides managing teams to counterbalance the fight against cybercriminals, he is focusing on various short and long-term research projects, ranging from small scale malicious campaigns through niche malware and file formats to in-depth investigations and threat actor attribution.

Robert is a long-time security researcher, working in IT - and especially in IT security - for most of his career. His previous experiences at companies such as Virusbuster, Sophos and Forcepoint enabled him to understand and respond to cybersecurity challenges on different levels.

PANEL DISCUSSION – THE CURSE OF THE FALSE POSITIVE

Evgeny Vovk
Kaspersky

Bio:

Evgeny joined Kaspersky in 2005 as a Project Manager in the Technology Alliances department, where he was responsible for managing the technical aspects of Kaspersky technologies' integrations with the solutions of selected OEM partners. He was a trusted advisor for partners, and drove the development of the technologies available for integration.

In 2013, Evgeny was invited to join Kaspersky's Threat Research team to head the External Benchmarking group. In this role, Evgeny was responsible for handling the full scope of activities related to independent testing. This included presenting Kaspersky's position on issues in the independent testing industry and discussing these with industry experts and counterparts, managing stakeholder expectations of Kaspersky's participation in independent tests, working on feedback with Kaspersky's malware analysts and experts from test institutes, creating private test methodologies and reviewing the existing methodologies of test labs.

Since 2017, Evgeny has led the External Benchmarking and Technology Positioning team, with additional responsibilities of supplying new media materials about Kaspersky's technologies, as well as co-participation in responding to inquiries from industry analysts.

Evgeny takes part in the Anti-Malware Testing Standard Organization (AMTSO) activities since 2013, including works over the Testing Protocol Standard, guidelines, etc.

Evgeny holds a master's degree in computer science and after graduation, worked as an IT security engineer, and head of an IT department before joining Kaspersky.

Vanja Svajcer
Cisco

Bio:

Vanja Svajcer works as a Technical Leader at Cisco Talos. He is a security researcher with more than 20 years of experience in malware research and detection development. Prior to joining Talos, Vanja worked as a Principal Researcher for SophosLabs and led a Security Research Team at Hewlett Packard Enterprise.

Vanja enjoys tinkering with automated analysis systems, reversing binaries and analysing mobile malware. He thinks time spent scraping telemetry data to find indicators of new attacks is well worth the effort. He presented his work at conferences such as Virus Bulletin, RSA, CARO, AVAR, BalcCon and others.

In his free time, he is trying to improve his acoustic guitar skills and often plays basketball, which at his age is not a recommended activity.

PANEL DISCUSSION – THE CURSE OF THE FALSE POSITIVE

Righard Zwienenberg
ESET

Bio:

Zwienenberg started dealing with computer viruses in 1988 after encountering the first virus problems at the Technical University of Delft. His interest thus kindled and studied virus behavior and presented solutions and detection schemes ever since. Initially starting as an independent consultant, in 1991 he co-founded CSE Ltd. In November 1995 Zwienenberg joined the Research and Development department of ThunderBYTE. In 1998 he joined the Norman Development team to work on the scanner engine. In 2005 Zwienenberg took the role of Chief Research Officer. After AMTSO – Anti Malware Testing Standards Organization - was formed, Zwienenberg was elected as president. He is serving on the board of AVAR and on the Technical Overview Board of the WildList. In 2011 Zwienenberg was looking for new opportunities and started as a Senior Research Fellow at ESET. In April 2012 Zwienenberg stepped down as President of AMTSO to take the role as CTO and later as CEO. In 2016 he rejoined the AMTSO board for another two-year run. He also is the Vice Chair of the Executive Committee of IEEE ICSG. In 2018, Zwienenberg joined the Europol European Cyber Crime Center (EC3) Advisory Group as an ESET representative.

Zwienenberg has been a member of CARO since late 1991. He is a frequent speaker at conferences – among these Virus Bulletin, EICAR, AVAR, FIRST, APWG, RSA, InfoSec, SANS, CFET, ISOI, SANS Security Summits, IP Expo, Government Symposia, SCADA seminars, etc. - and general security seminars. His interests are not limited to malicious code but have broadened to include general cybersecurity issues and encryption technologies over the past years.

Eddy Willems
G DATA

Bio:

Eddy Willems is a worldwide known cyber security expert from Belgium. He is a board member of 3 security industry organizations, EICAR, AVAR and LSEC, and is the resident Security Evangelist at G DATA Cyberdefense.

He became a founding member of EICAR in 1991, one of the world's first security IT organizations. Over the years he has served in many extra roles in different security industry organizations. Several CERTs, press agencies, print and online publications and broadcasting media, for example CNN, use his advice regularly. In October of 2013, he published his first book in Belgium and the Netherlands, entitled 'Cybergevaar' (Lannoo). A German translation followed afterwards and an English translation and update, Cyberdanger (Springer), was published in 2019. He is also co-author of the Dutch SF cyberthriller 'Het Virus' published in 2020. Eddy is a known inspiring speaker and is giving lectures and presentations (including TEDx) worldwide for a very diverse audience from children to experts.

PANEL DISCUSSION – THE CURSE OF THE FALSE POSITIVE

Samir Mody
K7 Computing

Bio:

Samir Mody graduated from the University of Oxford in 2000 with a First-Class Masters degree in Chemical Engineering, Economics and Management. He spent over 9 years at Sophos UK, the final 3 as Threat Operations Manager of SophosLabs. Since August 2010 he has been running K7 Labs in Chennai, India. Samir has actively contributed to the IEEE Taggant System project and other industry collaborations such as AMTSO and CTA. He has co-authored and/or presented papers and participated in panel discussions at various international security conferences (EICAR, VB, AVAR). Samir's interests include reading (philosophy, politics, history, literature, and economics), sport and classical music.

AVAR

Association of anti Virus Asia Researchers

AVAR exists to prevent the spread of cyber threats by fostering international cybersecurity collaboration

The AVAR Platform

Knowledge Center

Professional Development

Networking & Partnering

Conferences & Presentations

Product Launches

Join AVAR Today!

Individual & Corporate Memberships Are Available

www.aavar.org

PANEL DISCUSSION – IS THE CISO THE NEXT NEW BOARD MEMBER?

Victor Keong
Cohesity

Bio:

Victor Keong, HBA (Ivey 1993) CISA, EMBA (Ivey 1999), CISSP, has close to 30 years of Infosec experience around the globe, bringing his rich tapestry of cross-border/cultural/deep technical perspectives from the data center to the cloud, and translating these key challenges to board-understandable priorities. Victor is Cohesity's very first APJ's Field CISO, where he brings both innovative and empathetic perspectives to challenges and stay-awake issues for CISOs in the region. Prior to joining Cohesity, Victor was Cisco Systems' and Checkmarx's inaugural Senior CISO Advisor for Asia Pacific, Japan & China.

At Cisco Victor brought his strategic skills, relationships and experience to help CISOs more effectively perform their role and to help Cisco understand the unique and difficult role of today's security professional. Some of Victor's projects have been helping the Enterprise CISOs navigate the myriad of technical challenges presented with securing the remote workforce. Also, the rush to digital transformation has brought unprecedented challenges to the CISOs on topics such as rapid cloud adoption, agile computing and DevSecOps, with Victor actively advising the CISOs in these uncharted territories.

Prior to returning to his native Singapore in 2010, Victor spent 17 years with Deloitte in Canada. From a functional perspective, Victor was an experienced partner (17 years as a partner) in Deloitte's Cyber Risk Services practice, where he held several senior roles in Deloitte's Cyber Risk Services' Global Executive Management Committee, including Asia Pacific Cyber Risk Services' Leader and Global Leader for IT Vulnerability Management. He helped built the Cyber Risk Services Practice at Deloitte into one of the pre-eminent security consulting practices in the world. One of Victor's most recent contributions was to build up the Deloitte Japan Cyber Risk Service practice, and made it one of the strongest Information Security practices in Japan. In the last 10 years in Asia, Victor has served several significant FSIs, including but not limited to : Standard Chartered Bank, Citibank (Asia), UOB, MUFJ (Tokyo), Toyota Finance, MayBank, Kasikorn Bank, Siam Commercial Bank and SGX.

Victor was also Deloitte's Lead Client Service Partner with (ISC)2 - Information Systems Security Certification Consortium - where he directed Deloitte's global certification program with (ISC)2 , culminating in 5000+ CISSPs globally within Deloitte, the largest among any professional services firm. As a result of Victor's involvement with (ISC)2, Victor was appointed to (ISC)2 's Americas Advisory Board, alongside luminaries in the Information Security community. Victor is also fluent in Mandarin and a sought-after speaker, and has spoken on various conferences, and often quoted in the media.

PANEL DISCUSSION – IS THE CISO THE NEXT NEW BOARD MEMBER?

Ashish Thapar
NTT

Bio:

Ashish brings more than 2 decades of Information Security experience to his role at NTT. He has been leading and managing security consulting teams across APJ region; spanning across multiple security practices including: Security Strategy; Threat & Vulnerability management; Governance, Risk and Compliance; ICS/OT Security, Payment Security; Incident Response; Digital Forensics; and Cyber Threat Intelligence.

Along with his vast leadership experience, he also top global domain certifications including CISSP, CISM, CISA, SANS GCFA, CCSK, CIPP/A, ISO 27001 LI and CDCP. In addition, he has also been an accredited PCI QSA, PFI and PA QSA for several years. He is an active speaker at numerous security industry events/seminars throughout Asia, including coverage on live TV programmes and radio/podcast interviews.

He also serves as a Lead Mentor and SME Panellist for Cybersecurity domain helping Singapore Cyber Security Agency (CSA), ICE71 and other organizations to help strengthen the overall cybersecurity ecosystem in the region.

Dr. Tan Kian Hua
PCCW Solutions Limited/Lenovo

Bio:

Dr. Tan Kian Hua is a proven solution leader in the field of cybersecurity regionally with records of success and made significant contributions. Well-versed with security governance and policies, lead and oversee to ensure all ICT security matters are conducted accordingly to the Singapore Government Manual ICT Security Policy.

During his six years with an MNC, he was chosen as a young leader and attended their leadership program. He spearheaded a team to build from scratch the first world-class defence cybersecurity infrastructure and rectified a cyberattack within one day – the market average is twenty-eight days.

Dr. Tan holds multiple professional certifications related to Cybersecurity and data privacy:

- FIP (International Association of Privacy Professionals)
- Certified Information Privacy Professional/ United States (CIPP/US)
- CIPM (Certified Information Privacy Manager)
- CISM (Certified Information Security Manager)
- CISA (Certified Information System Auditor)
- CDPSE (Certified Data Privacy Solution Engineer)
- CEH (Certified Ethical Hacker)

He is passionate about creating awareness of the importance of cybersecurity in all companies and continues to ensure a first-class standard for maintaining cybersecurity procedures.

PANEL DISCUSSION – IS THE CISO THE NEXT NEW BOARD MEMBER?

Vishal Sharma
Kroll

Bio:

A result driven professional with over 20 years of experience in IT and ITES industry. Experience in project management and process improvement with knowledge of Risk Management, Information Security, Business Continuity, IT Service support and Service Delivery. Have ability to translate business needs into process and technology requirements that support organizations business objectives to successfully manage all phases of IT projects from needs analysis and requirements definition to development and/ or vendor selection implementation, support and training. The last 17 years have been in the space of Information Security Risk Management covering the areas under Information Security Assessments, Risk Management, Cybersecurity, 27001 implementation (complete cycle), ISO22301, BCP/DR, IT General Computer Controls, Business Cycle Controls and exposure to SSAE16, SOC1, SOC2, GDPR, HIPAA, CMS and GLBA assessments Electronics graduate and PGDBM with relevant industry qualifications such as CISA, CISM, CRISC, LA ISO27001:2005, ITIL V3 Foundation. Have re-engineered processes and executed projects resulting in successful implementation of BS7799 and ISO27001 framework and certification.

Boris Hajduk
Tokopedia

Bio:

Boris Hajduk is CISO at Tokopedia, where the security team is responsible for securing more than 1% of Indonesia's GDP and more than 100m monthly active users. Prior to Tokopedia, he held several CISO positions where he built, led and matured global cybersecurity programs and teams for high-growth companies in industries ranging from e-commerce to banking and social networks across ASEAN, Russia, LATAM, UAE, Australia, France and Germany. Boris helped 3 global companies prepare for their IPOs, including a unicorn and a decacorn.

PANEL DISCUSSION – IS THE CISO THE NEXT NEW BOARD MEMBER?

Dennis Batchelder
AppEsteem

Bio:

Dennis Batchelder is the President of AppEsteem Corporation, where he's eradicating unwanted software while helping the software monetization industry thrive. He spent eight years at Microsoft, where he led their antimalware efforts to protect billions of customers through real-time antimalware products and services, industry partnerships, and continuous analysis of threat intelligence using machine learning and the cloud. Prior to Microsoft, Dennis owned the threat and security information management product lines as a Senior Vice President at Computer Associates, which he joined after founding, running, and selling them a network security product company. Dennis has worked for more than thirty years in the security industry holding various leadership roles in the US and India. He lives in Seattle, Washington. Dennis is the author of the Soul Identity series of techno-thriller novels.

AVAR

Association of anti Virus Asia Researchers

Enabling International Cyber Security Collaboration Since 1998

/avar-asia/ /avar_asia /aavar.org

www.aavar.org